中国南方电网
CHINA SOUTHERN POWER GRID

贵州电网公司计量自动化系统 3.0 建设（计量自动化系统分布式平台基础设施）技术规范书

CHINA SOUTHERN POWER GRID CO., LTD.

贵州电网有限责任公司

2025 年 2 月

目 录

1 总则

1.1 总体说明

本文件为“计量自动化系统分布式平台基础设施”的招标技术规范书（以下简称“技术规范书”）。

本技术规范书的最终解释权归贵州电网公司所有。

1.2 一般规定

1．本项目的整体项目为“贵州电网公司计量自动化系统 3.0 建设”，本项目为“计量自动化系统分布式平台基础设施”，本文件内容为“计量自动化系统分布式平台基础设施”的标准技术要求。

2．本次招标采购方为贵州电网有限责任公司（以下简称“贵州电网公司”），在本文中，具备所要求资质参与投标的供应商简称“投标方”，中标的投标方简称“中标方”，本项目建设单位为贵州电网公司。

3．本文件中提到的“集成商”，是指本项目中标方，负有软硬件整体集成的责任。

4．本文件中的相关术语，例如 Region（地域）、AZ（可用区）以及相关产品名称，主要是参考业界权威机构标准、主流云平台厂商通用术语，并且结合本项目建设需求制定。

5．投标方所提供的产品及服务应符合以下要求：

(1) 满足《中华人民共和国网络安全法》、《中华人民共和国密码法》、《中华人民共和国数据安全法》等国家法律法规；

(2) 满足电力行业信息安全等级保护基本要求（应用安全、数据安全、主机安全、网络安全等方面），等保要求为三级，满足《信息安全技术 网络安全等级保护基本要求》)(GB/T 22239-2019)第 3 级安全要求的安全通用要求和云计算安全扩展要求；

(3) 满足国家商用密码应用的相关要求，满足 GB/T 39786-2021 信息安全技术信息系统密码应用基本要求》第 3 级安全要求。涉及密码技术的安全设备或防护措施应达到《GB/T 37092 信息安全技术 密码模块安全要求》2 级及以上安全要求；

(4) 满足电力监控系统安全防护规定（国家发改委 27 号令）、电力监控系统安全防护总体方案等安全防护方案和评估规范（国能安全〔2015〕36 号），满足中国南方电网电力监控系统网络安全技术规范，满足电力监控系统安全防护评估要求；

(5) 严禁含有预置的安全漏洞、恶意代码，满足第三方测试、安全检测（含入网安全评测、源代码安全审查）、渗透测试等要求。

(6) 双方项目违约的处罚将在合同谈判中明确。

1.3 投标须知

1．技术规范书中提出的仅为最低限度的技术要求，并未对一切技术细节作出规定，也未充分引述有关标准和规范的条文，投标方应提供符合相关标准和本技术规范书标准以上的产品。本技术规范书所使用的标准如与国家、行业、公司以及投标方所执行的标准不一致时，按要求较高的标准执行。

2．投标方应仔细阅读包括本技术规范书在内的招标文件的所有条款，并根据技术规范书中的要求和范围进行技术方案的设计，提供的设备及技术方案应满足招标文件所规定的所有要求。

3．对于本技术规范书未提出但应标平台已具有的功能及技术性能指标，投标方可在其技术建议书中加以补充说明，并提供相关技术资料。如果投标方认为本技术规范书所描述的功能、性能等要求与目标平台要求有所不一致或部分要求不合理，可在响应原要求后给出建议方案。

4．对于应标平台中尚不具备或未达到相关要求的功能或性能，投标方在应答时须针对该项如实说明。投标方认为相关要求不合理的，应给出充分理由及合理的建议。投标方认为相关要求需要在现有产品基础上进一步实现或完善的，应给出实现相关技术要求的方案和进度计划。

5．投标方提供的产品必须是标准的，技术上是成熟的，所有产品应是全新的，具有先进结构，并能在中国境内安全使用(包括软件产品必须具有在中国境内的合法使用权)，符合环保要求。

6．投标方应依据本技术规范书的要求及推荐的技术方案提出详细的产品功能和报价清单。

7．投标方的报价清单内容应该包括本次招标范围内所要求的全部软硬件设备、材料及服务等。除已经明确说明由贵州电网公司另行采购和在报价清单中明确采购的设备、材料及服务外，其它在本项目建设中必须的但未列出的设备、材料及服务，投标方应予以补充，在清单中详细列出并报价，以保证满足招标平台的技术要求并正常运行。否则，相关软硬件设备、材料及服务等的费用被视为已包含在报价中或由投标方免费提供。

8．投标方的投标文件应以中文简体编写，所有的计算、说明和图纸等均应采用国际单位。

9．投标方应保证对本次招标的所有技术说明文件保密，在招标前和招标后不得向其他单位公布招标项目单位的有关材料。

10．本技术规范书的解释权属于贵州电网公司。未经贵州电网公司同意，任何个人和单位对技术规范书所作的任何修改均无效。在未经双方商定作为订货合同技术附件之前，贵州电网公司保留对本技术规范书进行修改的权利，投标方可以提出变更的意见和建议。招投标双方签订合同之后，贵州电网公司有权提出且投标方有责任接受因国家、行业、上级主管单位等的规范、标准和规程等发生变化及与相关系统接口要求改变所产生的一些补充要求。具体事项由招投标双方共同商定。

11．本技术规范书在内容或技术指标上如果存在错误(包括拼写、印刷错误)，投标方应及时提出并要求贵州电网公司澄清，经贵州电网公司确认后对错误内容进行修正。

12．针对本次招标的一切有效的书面通知、修改及补充，都是招标文件不可分割的部分，与招标文件具有同等法律效力。

13．技术规范书经招投标双方确认后作为合同的附件，与合同正文具有同等的法律效力。本技术规范书的未尽事宜，由招投标双方在合同技术谈判时协商确定，或以其它形式补充。

1.4 技术应答要求

1．投标方提供的技术投标书必须包括点对点应答文件和技术建议书两部分作为应答。

2．投标技术文件格式参照附件编制，点对点应答文件单独形成文件，编制内容详见《附件 2 点对点应答文件编制要求》，包括但不限于已列出内容。投标方提供的点对点应答文件应对本技术规范书每一章的每一项逐项回答，存在差异的内容，投标方必须详细标明技术差异。

3．投标方提供的技术建议书至少应包括技术文件评价索引表、技术差异表、总体技术方案、关键指标技术响应、详细技术方案、安全技术方案、工程进度计划及保障措施、实施方案、售后服务承诺、技术研发实力、其他技术附件等。根据《附件 1：技术建议书编制要求》编写，包括但不限于已列出内容。

4．投标方注意：投标方提供的技术建议书不应是投标方投标产品的通用产品说明，

应充分突出其满足或优于本技术规范书的详细技术方案。为便于评标专家评标，应根据《附件 1：技术建议书编制要求》第一章技术文件评价索引表，充分总结投标产品的技术特征及优于招标技术规范书的主要技术特点，编写技术优势内容，在其他章节中对应编写技术建议书内容。

5．投标方提供的技术建议书的内容与本技术规范书存在差异的内容，投标方必须根据《附件 1：技术建议书编制要求》第二章技术差异表的要求详细标明技术差异。即使无偏差，也应列出其实现方式，并附有详细、全面的技术资料，否则其将被认作没有回答。

6．投标方应在技术建议书中具体说明所建议的技术方案、系统配置符合的有关标准(包括国际、国内标准和专用标准)，并附上相应的说明和技术资料。技术建议书中的每个软件的型号/部件号必须逐一说明。对每个单项产品，投标方必须提供原厂商的正式技术指标说明材料。投标方认为需特殊说明的部分应附有详细的技术资料，否则由于评标理解的不同，产生的后果由投标方负责。

7．投标方也可推荐能满足招标文件要求的类似的或更优的产品和方案，但投标方必须详细标明技术差异（详见《附件 1：技术建议书编制要求》第二章技术差异表）。未在技术差异表中说明的条款意味着投标方认可其所提供的软硬件设备、产品、技术参数、技术指标及服务等的相应部分完全符合或高于本技术规范相应的要求，投标方中标后除非经过贵州电网公司书面同意，否则不得以任何理由提供低于本技术规范要求的相应的设备、产品及服务等。

8．投标方在技术建议书中，按本技术规范书中所提的技术及集成等要求，对涉及到的主要产品、技术及服务，提供详细的性能参数和技术说明。投标方亦可根据自己的产品技术性能具体情况，在技术建议书中提出建议，并附详细资料和说明。

9．投标书对于需提供具体设计或实现方案的应答，需要提供详细的体系框图、功能细节、实现技术，相关功能均需给出计算方法和软件实现的流程框图。

10．投标方应提供工程总体兼容性要求承诺书、虚拟化技术平台软件原厂针对硬件设备的兼容性、分布式平台软件原厂针对硬件设备的兼容性证明、分布式平台厂商技术路线承诺书、安全自主可控软件承诺书、分布式平台软件原厂合法授权书、虚拟化技术平台软件原厂合法授权书、硬件设备原厂针对本项目出具的合法授权书、分布式平台软件原厂技术服务承诺书、硬件设备原厂针对本项目出具的技术服务承诺书等，包括但不

限于已列出内容，并按照附件中指定的格式填写。

11．投标方应随其投标书一起提供足够详细和清晰的产品说明，以便能够与本招标文件中的技术条款进行完整和切实的比较。这些产品说明应简要说明系统的设计特点，同时对与技术规范书要求有差异或偏差之处进行准确说明。除非经贵州电网公司同意，系统的最终设计应按照这些产品说明的所有详细说明进行。

12．投标文件中若出现相互矛盾或不一致的内容，以有利于贵州电网公司的内容为准。

13．在必要时投标方须在贵州电网公司要求下提供应标平台的演示。

2 应遵循的主要标准

1．除本技术规范书特别规定外，投标方所提供的设备均应按照国际、国家、行业、公司标准、规范、规定进行设计、制造、检验和安装。所用的标准必须是其最新版本。除非另作特别规定，所有合同设备，包括中标方从他处获得的全部设备或附件，都必须满足最新版本的相关标准，包括在投标时已生效的任何修改和补充。如果投标方选用标书规定以外的标准时，需提交与这种替换标准相当或优于标书规定标准的证明，供贵州电网公司确认。

2．本技术规范书主要引用或参照了以下标准和规范，投标的设备和产品应符合本技术规范及下列标准和规范的要求。

(1) 《中华人民共和国网络安全法》

(2) 《中华人民共和国密码法》

(3) 《中华人民共和国数据安全法》

(4) 《“十四五”数字经济发展规划》（国发〔2021〕29 号）

(5) 《电力监控系统安全防护规定》（国家发展和改革委员会 27 号令）

(6) 《国家能源局关于印发电力监控系统安全防护总体方案等安全防护方案和评估规范的通知》（国能安全[2015]36 号）

(7) 《计量发展规划（2021—2035 年）》（国发〔2021〕37 号）

(8) 《关于完善能源绿色低碳转型体制机制和政策措施的意见》

(9) 《关于加强国家现代先进测量体系建设的指导意见》

(10) 《商用密码应用安全性评估管理办法》（国家密码管理局第 3 号令）

(11) 《信息安全技术 网络安全等级保护基本要求》（GBT 22239-2019）

(12) 《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）

(13) 《信息安全技术 网络安全等级保护测评要求》

(14) 《电力监控系统网络安全防护导则》（GB/T 36572-2018）

(15) 《信息安全技术 信息系统密码应用基本要求》（GB/T 39786-2021）

(16) 《信息安全技术 密码模块安全要求》（GB/T 37092-2018）

(17) 《信息安全技术 云计算服务安全指南》（GB/T 31167-2023）

(18) 《信息安全技术 信息系统密码应用设计指南》（GB/T 43207-2023）

(19) 《信息安全技术 密码模块安全检测要求》（GB/T 38625-2020）

(20) 《信息安全技术 IPSec VPN 技术规范》（GB/T 36968-2018）

(21) 《信息安全技术 密码设备应用接口规范》（GB/T 36322-2018）

(22) 《信息安全技术 智能密码钥匙应用接口规范》（GB/T 35291-2017）

(23) 《信息安全技术 信息系统灾难恢复规范》（GB/T 20988-2007）

(24) 《密码设备应用接口规范》（GM/T 0018-2023）

(25) 《IPSec VPN 技术规范》（GM/T 0022-2023）

(26) 《IPSec VPN 网关产品规范》（GM/T 0023-2023）

(27) 《SSL VPN 技术规范》（GM/T 0024-2023）

(28) 《SSL VPN 网关产品规范》（GM/T 0025-2023）

(29) 《智能密码钥匙技术规范》（GM/T 0027-2014）

(30) 《密码模块安全技术要求》（GM/T 0028-2014）

(31) 《服务器密码机技术规范》（GM/T 0030-2014）

(32) 《信息系统密码应用基本要求》（GM/T 0054-2018）

(33) 《南方电网公司“十四五”发展规划和 2035 年远景目标展望》

(34) 《南方电网公司“十四五”市场营销规划》

(35) 《南方电网公司“十四五”数字化规划》

(36) 《南方电网公司“十四五”电能量数据深化应用规划》

(37) 《南方电网公司发展战略纲要（2019 年版）》

(38) 《公司数字化转型和数字南网建设行动方案》

(39) 《南方电网新型电力系统白皮书》

(40) 《南方电网服务碳达峰、碳中和工作方案》

(41) 《南方电网公司现代供电服务体系建设工作方案》

(42) 《南方电网公司数据安全管理工作指引（2023 年版）》

(43) 《南方电网公司网络安全合规库（2022 年修订版）》

(44) 《南方电网公司 IT 主流设备安全基线技术规范》

(45) 《南方电网公司涉密事项界定范围表》（南方电网办[2016]13 号）

(46) 《南方电网公司数据共享开放指导意见（试行版）》（信息[2017]51 号）

(47) 《重要应用与数据灾难备份系统建设技术导则》

(48) 《南方电网公司营销项目预算标准、准入条件与项目命名规范（2023 版）》

(49) 《中国南方电网有限责任公司营销项目管理办法》

(50) 《关于印发新一代计量自动化主站试点建设工作方案的通知》（办市场〔2022〕37 号）

(51) 《关于印发南方电网公司新一代智能量测体系建设指导意见的通知》（南方电网市场〔2022〕12 号）

(52) 《中国南方电网电力监控系统网络安全技术规范》（Q/CSG 1204099）

(53) 《中国南方电网有限责任公司企业标准 数字化总体技术导则（试行）》（Q/CSG 1210073-2024）

(54) 《计量自动化系统 3.0 技术架构设计说明书》

(55) 《计量自动化系统 3.0 统一基座设计说明书》

(56) 《计量自动化系统 3.0 安全防护方案》

(57) 《关于印发南方电网公司计量自动化系统及新型电力负荷管理系统网络安全防护专项提升工作方案（2024-2025 年）》

(58) 《2024 年贵州电网有限责任公司计量自动化系统 3.0 建设项目初步设计报告》

(59) 《2024 年贵州电网有限责任公司计量自动化系统 3.0 建设项目可行性研究报告》

由于国家、行业、南方电网公司的相关技术规范还在逐年完善中，投标方须承诺在“贵州电网公司计量自动化系统 3.0 建设”项目竣工前无条件的对系统进行改进，以便适应相关技术规范发展的最新要求。

3 项目概述

3.1 项目背景

以习近平新时代中国特色社会主义思想为指导，践行“人民电业为人民”的企业宗旨和“为客户创造价值”的服务理念，按照《南方电网公司“十四五”发展规划和2035年远景目标展望》、《南方电网服务碳达峰、碳中和工作方案》、《南方电网新型电力系统白皮书》、《南方电网现代供电服务体系建设工作方案》、《南方电网公司“十四五”数字化规划》、《贵州电网有限责任公司“十四五”电网发展规划》和《贵州电网公司“十四五”营销技改与电能计量规划》等相关部署要求，结合网、省公司对数字电网的建设要求，运用“解放用户”实践方法论，构建数字电网的基础系统，充分发挥计量数据在电网企业的核心作用，加快省级计量自动化主站系统的技术演进和业务发展，构建全息感知、随需采集、灵活开放、智能高效、安全可靠的计量自动化系统3.0，满足高频、全量、实时计量数据的高效采集、集中管理和灵活应用，服务国家“碳达峰、碳中和”战略，服务新型电力系统建设，支撑现代供电服务体系前中后台建设。

近年来，南方电网公司全力推进数字化转型和数字电网建设，催生高质量发展新动能、新优势。贵州电网公司通过计量自动化系统服务新能源发展，通过采集光伏等分布式项目电量，实现新能源规范计量，促进新能源规范化发展。对大数据中心、工业互联网、5G、人工智能、电力北斗应用等“新基建”领域用电情况进行监测、分析，不断调优综合能源计量支持和精益服务能力，为区域新能源调度与用户一揽子节能规划提供支撑，共创绿色清洁新能源。此外，贵州电网公司还创新计量管理模式，深化电能量数据应用。整合数据资源，以数据采集管理及数据业务应用为支点打造“电能量数据应用工作平台”，实现运营数据全管控、用户状态全感知、专业管理全在线的新工作模式，推动计量管理向平台化、数字化转变。

目前，贵州电网公司省级计量自动化主站系统统一部署在贵阳观水路机房中，支撑全省2014万用户电能量数据的统一采集、统一处理、统一存储和统一应用。省级计量自动化主站系统作为生产系统，不仅需要支撑一线生产运行，同时需要构建服务共享和数据驱动能力，聚合多方数据，在营销服务、生产运行、新型业务、社会经济等方面充分挖掘数据价值，拓展多方应用场景。对于贵州电网公司来说，充分挖掘数据价值，是管理优化、效率提升的必由之路。

现有省级计量自动化系统在基础支撑能力、系统采集能力、数据开放共享、数据赋能业务等方面存在掣肘和瓶颈，无法支撑面向政府、面向公司、面向客户的业务发展，亟需开展架构优化升级提升计量自动化主站的系统支撑能力。同时，计量自动化主站系统作为全省计量业务数据采集、计算、存储、应用、发布的核心生产系统之一，其稳定、可靠运行是保证全省计量及营业抄核收业务正常开展的基础，也是服务好政府、服务好公司、服务好客户的重要支撑。该系统和设备高度集中，生产运行高度依赖数据库一体机，且未开展数据备份系统和应用容灾系统建设。如果该机房出现网络出口异常、机房停电等极端异常情况，计量自动化主站系统将无法对外提供服务，影响全省计量业务乃至营业抄核收业务，将造成无可挽回的重大损失。

综上分析，亟需开展计量自动化系统 3.0 建设，把握“云大物移智链”为代表的新技术带来新机遇，满足为用户提供可靠、便捷、高效、智慧的现代供电服务体系建设提出新要求，支撑以新能源为主体的新型电力系统建设催生新业务，全面提高业务支撑能力和数据共享能力，满足安全防护技术规范要求，保障极端环境下系统的稳定可靠运行。

3.2 项目内容

按照“一主两域、云边协同”的总体设计思路，服务国家“碳达峰、碳中和”战略，服务新型电力系统建设，支撑现代供电服务体系前中后台建设；应用先进的数字化技术，全面提升弹性伸缩、敏捷迭代的架构支撑能力，全面提升广泛接入、灵活定制的数据采集能力，全面提升多源融合、开放共享的应用创新能力，构建“随需采集、灵活开放、智能高效、安全可靠”的计量自动化系统 3.0，高效满足未来业务快速迭代需求，充分释放电能量数据在营销服务、电网运行、新兴业务和经济发展等领域的价值创造，有力支撑公司实现高质量发展。

3.2.1 贵州计量自动化系统 3.0 总体架构

计量自动化系统 3.0 建设属于数字化转型中的数字电网建设，计量自动化系统 3.0 从量测装置、通信、平台及应用部署、数据流线及时性要求等方面均满足数字化转型的指导原则要求，计量自动化系统 3.0 采用网、省两级级部署，采用一主两域、云边协同方式，划分为数据分析域和采集监控域，分别基于调度云棠下延伸节点和边缘计算集群部署。

为保障计量自动化基础核心功能安全稳定可靠运行，将海量数据挖掘分析等占用大量存储计算资源的功能剥离出来，计量自动化系统 3.0 按照采集监控域和数据分析域设

计。采集监控域主要承载生产运行及实时数据共享等业务，数据分析域主要承载海量数据价值挖掘及非实时数据共享等业务。两个域软硬件独立部署，通过数据和应用交互实现计量自动化主站全部功能，并通过统一人机交互界面提供给公司各级人员访问使用。计量自动化系统 3.0 主站总体架构如下：

图 3-1 总体架构

采集监控域基于统一基座模式建设。基座主要对数据模型、算法规则、数据交互进行统一，实现基础的数据存储计算服务标准化，满足基础能力复用要求，并基于基座开展相关业务应用建设，部署在贵州计量检定中心机房。

数据分析域基于能力开放平台和交互共享平台建设。数据分析域能力开放实现多源数据融合，提供基础能力、存储能力、计算能力和服务能力四个层次的能力开放，全面支撑各专业部门、基层单位开展电能量数据创新应用，部署在广州棠下数据中心。

3.2.2 本项目建设范围

(1) 采集监控域分布式平台及基础软硬件环境建设

安全接入区：安全接入区部署边缘集群软硬件资源虚拟化技术平台，支持容器化部署，提供微服务支撑框架、消息队列、内存数据库、中间件服务、安全服务、商用密码服务、配套软件、服务器、网络设备、安全及配套设备等，并在安全接入区部署代理程序（本代理程序负责将接入区态势感知探针采集信息跨隔离推送到安全Ⅱ区部署的态势感知主站系统等）。

安全Ⅰ区：安全Ⅰ区部署控制子系统的相关安全服务、商用密码服务、配套软件、服务器、网络设备、安全及配套设备等软硬件资源设备；

安全Ⅱ区：安全Ⅱ区部署边缘集群软硬件资源虚拟化技术平台，支持容器化部署，提供微服务支撑框架、消息队列、内存数据库、中间件服务、安全服务、商用密码服务、配套软件、服务器、网络设备、安全及配套设备等，并在安全Ⅱ区部署子站系统（本系统能够识别来自安全接入区、安全Ⅰ区Ⅱ区的态势感知探针推送的日志，识别分析102规约流量，及相关界面展示等）；

安全Ⅲ区：安全Ⅲ区部署边缘集群软硬件资源分布式平台，提供云平台底座、基础设施服务、数据库服务、中间件服务、数据计算组件、能力开放中心、云安全服务、商用密码服务、配套软件、服务器、网络设备、安全及配套设备等，并在安全Ⅲ区部署子站系统（本系统能够识别来自安全Ⅲ区的态势感知探针推送的日志，及相关界面展示等）。

(2) 采集监控域系统集成实施

软硬件设备安装含设备上架、上电、配置和相关实施材料的购置等等，完成采集监控域各区计量自动化系统分布式平台、虚拟化技术平台及基础软硬件与主站系统采集监控域业务应用联调和运行优化等，完成云边协同、跨区跨域数据同步等工作，完成与贵州现有计量自动化系统的设备及通信工程设备接线及联调工作，完成与调度态势感知系统采集装置接入，完成与现有系统的连线和联调，通过租户+资源隔离的形式实现生产环境与开发、测试等环境的隔离，完成相关部署实施等工作。

(3) 采集监控域系统测试

配合完成第三方测试、等保测评及安全防护评估、商用密码应用安全性评估（含商用密码方案评审）、安全检测（含入网安全评测、源代码审计）、渗透测试、电力监控系统安全风险评估等安全评测，云边协同技术验证及建设质量评价，并负责完成边缘集群（采集监控域）涉及到的安全问题整改，满足安全测评相关要求。

3.2.3 本项目与关联项目的关系

本项目（计量自动化系统分布式平台基础设施）工作界面主要包括中标方与主站应用功能建设、机房及通信、系统测试服务等标段的界面；与主站应用功能建设的工作界面包含硬件设备采购及安装集成、软件系统、大数据计算及存储、微服务软件、项目实施、安全防护及测试、发布管理等内容；与机房及通信的工作界面包含机房基础环境部署、设备上架及接线以及上电、测试及验收、系统启停控制、安全防护及测试等内容；与系统测试服务的工作界面包含第三方测试、网络安全等级评测、入网安全评测、源代

码安全审查、商用密码应用安全性评估（含商用密码方案评审）、电力监控系统安全防护评估、渗透测试等内容。详细的工作界面内容见章节 3.3。

3.3 本项目与关联项目的工作界面

本项目（计量自动化系统分布式平台基础设施）工作界面主要包括中标方与主站应用功能建设、机房及通信、系统测试服务等标段的界面。

其中主站应用功能建设包括计量自动化系统 3.0 采集监控域主站应用功能的开发，以下统称为“主站应用功能建设”；系统测试服务包括项目测试服务及云边协同技术验证及质量评价研究服务，以下统称为“系统测试服务”。

3.3.1 与主站应用功能建设的工作界面

序号	工作项	本标段的工作内容	主站应用功能建设中标方的工作内容	备注
1.	硬件设备采购及安装集成	(1)在中标后30天内在业主指定机房中完成开发测试环境搭建。中标方负责提供开发测试环境所需的资源，环境应采用风冷的制冷模式，并提供不少于生产环境的20%的可用资源，包括但不限于服务器、交换机、云平台基础组件、协同开发平台等全套的软硬件环境，软件版本应与生产环境保持一致。中标方应负责提供开发测试环境搭建所需的耗材，并负责实施和配置等工作，均由中标方自行评估并在投标文件明确罗列，开发环境应能保证主站应用功能建设开发厂家在系统上线前的正常开发、测试等工作。并且承诺后续可以免费迁移至计量检定中心机房。 (2)负责搭建一套可以支撑业务人工智能应用的大模型环境，支持多模态、图像识别、语音识别、语义识别等，协助贵州电网公	(1)施工前提供参数配置、数据库划分、操作系统配置、网络需求等基础软硬件环境部署所需前置需求。 (2)提供主站应用功能建设在采集监控域分布式平台建设工程采购清单以外所依赖的必须的软件或硬件，负责安装部署调试联调，满足安全相关的要求。	

序号	工作项	本标段的工作内容	主站应用功能建设中标方的工作内容	备注
		司开展大模型的业务应用训练等工作。 (3)负责按照项目要求提供本项目需要的硬件设备。 (4)结合产品特性，根据业务建设需求及软件开发需求，完成基础软硬件环境安装、部署、配置及联调工作。		
2.	软件系统	(1)负责提供本项目需要的采集监控域安全III区分布式平台相关组件。 (2)负责提供本项目需要的各安全分区（安全II区、安全接入区）虚拟化技术平台、微服务平台、Kafka等数据传输的相关组件等。 (3)负责提供本项目需要的安全I区相关组件。	(1)主站应用功能建设中标厂家提供采集监控域软件功能对应的软件系统含源代码。 (2)主站应用功能建设中标厂家提供数据分析域软件功能对应的软件系统含源代码。 (3)主站厂家应按照“应用尽用、可用尽用”原则充分利用本次采购软件组件实现主站应用功能。	
3.	大数据计算及存储	(1)负责提供本项目采购的大数据计算、存储相关的硬件资源、软件组件，相关参数及性能指标详见本技术规范。 (2)对计算过程提供调度、管理、监控工具。	(1)负责调用大数据计算组件，完成业务数据的分析应用。 (2)负责保证业务数据计算的性能，包括计算的实时性、准确性。 (3)借助计量自动化系统分布式平台组件负责对大数据计算性能的监控，提供性能指标分析数据。	
4.	微服务软件	(1)负责建设及提供微服务应用架构。 (2)负责保证微服务架构的稳定性及性能。 (3)负责提供微服务应用开发、测试、发布、控制工具。	(1)负责根据平台厂商提供的微服务架构定制应用开发。 (2)负责微服务接口标准代码调用的定义。 (3)负责使用微服务应用进行主站应用功能开发、测试、发布。	
5.	项目实施	(1)负责部署本项目相关的软硬件现场集成实施、测试、验收。 (2)协助主站应用功能建设进行系统业务调优。	(1)负责主站应用功能建设业务系统的部署、测试、集成验证。 (2)负责系统实施阶段的架构调优、网络优化、主站软件	

序号	工作项	本标段的工作内容	主站应用功能建设中标方的工作内容	备注
		(3)实施阶段派驻计量自动化系统分布式平台云计算、数据库、大数据等专业技术专家，全程参与技术方案的编制，按照行业最佳实践经验给予主站应用功能建设开发单位软件设计技术指导。协助主站应用功能建设厂家完成数据库的数据库规划和数据模型建设。 (4)负责完成与现有系统、数据分析域的设备连线、配置和联调，若现有系统、数据分析域设备缺少通信的模块等辅助材料，也含在中标方的供货范围之内，中标方负责与现有系统、数据分析域的通信通道联调并保障系统的正常运行。 (5)负责在安全III区提供各安全分区的“云计算平台资源监测信息及配置信息、虚拟机资源监测信息、微服务监测信息、容器资源监控信息、安全管理中心监测信息”等，并提供接口实现与主站应用功能建设厂家进行内部数据交互，配合主站应用功能建设厂家完成接口联调工作。	与平台的兼容性优化等优化工作，负责项目实施阶段，主站应用功能建设相关全部实施工作，包括两域实施工作、现有系统与新系统实施工作、专项实施工作。 (3)负责主站应用功能出厂验收，配合贵州电网公司完成现场验收、竣工验收等验收工作。 (4)负责完成接口联调工作，实现内部数据交互。	
6.	安全防护及测试	(1)负责本项目相关的安全防护工作。 (2)配合第三方测试、等保测评及安全防护评估、商用密码应用安全性评估（含商用密码方案评审）、安全检测（含入网安全评测、源代码审计）、渗透测试、电力监控系统安全风险评估、云边协同技术	(1)负责主站应用功能建设系统相关的安全防护工作。 (2)配合第三方测试、等保测评及安全防护评估、商用密码应用安全性评估（含商用密码方案评审）、安全检测（含入网安全评测、源代码审计）、渗透测试、电力监控系统安全风险评估、云边协同技术验证及建设质量评	

序号	工作项	本标段的工作内容	主站应用功能建设中标方的工作内容	备注
		验证及建设质量评价研究服务，并负责完成问题整改。 (3)提供计量自动化系统商用密码应用方案采集监控域分布式平台建设部分。 (4)提供密码服务管理平台、服务器密码机、数据脱敏、数据水印等密码软硬件的功能、接口供主站应用功能建设厂家使用，以满足主站在应用和数据安全的密码应用安全建设要求。	价研究服务，并负责完成问题整改。 (3)提供计量自动化系统商用密码应用方案主站应用功能建设部分（含数据分析域和采集监控域）。 (4)本系统开发工作应遵循南网相关要求，确保源代码符合安全及规范管控要求。 (5)全面适配本项目采购的安全、可控、可靠基础软硬件环境进行开发及实施。	
7.	发布管理	(1)提供版本发布管理工具。 (2)提供代码审核工具。	(1)提交主站应用功能建设业务系统源代码。 (2)提交业务发布申请。 (3)提供发布代码供建设单位审核。 (4)负责发布后的运行监控。	建设单位负责组织审核承建单位的源代码。

3.3.2 与机房及通信的工作界面

序号	工作项	本标段的工作内容	机房及通信建设中标方的工作内容
1.	机房基础环境部署	(1)配合本项目软硬件设备的到货验收工作。 (2)负责本项目的软硬件资源部署规划工作，提供平台软硬件的施工图草图。 (3)配合机房及通信的施工，保障本项目软硬件资源在机房施工完成前的完整性、可用性。	(1)负责通信机房、自动化机房的基础环境部署工作。 (2)协助采集监控域分布式平台建设工程开展软硬件资源部署工作，明确机柜的承重、散热、供电等必要指标，提供机房的整体环境施工方案。
2.	设备上架、接线、上电	(1)负责自动化机房至通信机房之间的尾纤接线工作；（从自动化机房边界防火墙至通信机房路由器）。 (2)负责本项目所有设备的搬运、清洁、安装上架、设备间接线（含网线及光纤的接线）、上电、标签标识工作，确保设备稳定可靠运行。	(1)负责自动化机房及通信机房内的机柜间综合布线工作（含自动化机房、棠下机房）。 (2)负责机柜内六类电口网线、25GE以内光纤线缆的供货。 (3)负责综合数据网、调度数据网接入交换机对应的配线架，无线公网路由器、北斗服务器对应的配线架，上述配线架以外的接线工作。

序号	工作项	本标段的工作内容	机房及通信建设中标方的工作内容
		(3)配套机房工程的综合布线不满足本项目中标单位产品部署要求的，需本项目中标方按照配套机房工程的建设标准要求进行综合布线，并含柜间和柜内的全部材料及实施工作。 (4)负责从综合数据网、调度数据网接入交换机对应的配线架及无线公网路由器、北斗服务器对应的配线架到各区域边界防火墙所有设备间跳线、调试配置等工作，提供实施跳线所需的材料。	(4)自动化机房内每个服务器机柜按照48芯光口，24个电口配置，汇聚至本列的网络列头柜，网络列头柜采用24芯室内多模光缆汇聚至区域汇聚配线柜（F4），区域汇聚配线柜（F4）采用室内多模光纤与原自动化机房汇聚配线柜（B16）互联。
3.	测试及验收	(1)负责本项目软硬件设备的现场功能测试、验收工作。 (2)负责开展内部网络联通测试、验收工作。 (3)协助机房及通信开展外部网络联通测试、验收工作。	(1)负责机房及通信外部网络联通测试、验收工作。 (2)协助开展内部网络联通测试、验收工作。
4.	系统启停控制	(1)负责本项目的系统启停控制，在机房断电，UPS即将失效等极端情况下，通过计划性下电关闭各集群和软硬件，时间不可超过50分钟，并保证数据不丢失。在系统可以恢复运行后，通过计划性上电开启各集群和软硬件，时间不可超过40分钟。	(1)负责机房的UPS功率满足系统启停时候设备产生的峰值功率。
5.	安全防护及测试	(1)本项目相关的安全防护工作。 (2)配合第三方测试、等保测评及安全防护评估、商用密码应用安全性评估（含商用密码方案评审）、安全检测（含入网安全评测、源代码审计）、渗透测试、电力监控系统安全风险评估、云边协同技术验证及建设质量评价研究服务，并负责完成问题整改； (3)提供计量自动化系统采集监控域分布式平台的商用密码应用方案内容。	(1)机房及通信相关的安全防护工作。 (2)配合第三方测试、等保测评及安全防护评估、商用密码应用安全性评估（含商用密码方案评审）、安全检测（含入网安全评测、源代码审计）、渗透测试、电力监控系统安全风险评估，并负责完成问题整改。 (3)提供计量自动化系统机房及通信部分的商用密码应用方案内容。

3.3.3 与系统测试服务的工作界面

序号	工作项	本标段的工作内容	系统测试服务方的工作内容
1.	第三方测试	须配合系统测试方开展第三方测试工作，提供必要的设备、软件清单，并负责完成问题整改。	负责开展第三方测试工作，提供必要的测试结果、整改意见，并负责对整改后的系统进行复测。
2.	网络安全等级评测	须配合系统测试方开展网络安全等级评测工作，提供必要的设备、软件清单，并负责完成问题整改。	负责开展网络安全等级评测（含系统侧、平台侧）工作，提供必要的测试结果、整改意见，并负责对整改后的系统进行复测。
3.	入网安全评测	须配合系统测试方开展入网安全评测工作，提供必要的设备、软件清单，并负责完成问题整改。	负责开展入网安全评测工作，提供必要的测试结果、整改意见，并负责对整改后的系统进行复测。
4.	源代码安全审查	须配合系统测试方开展源代码安全审查工作，提供必要的设备、软件清单，提供必要的软件程序源代码或源代码安全审查证明报告，并负责完成问题整改。	负责开展源代码安全审查工作，提供必要的测试结果、整改意见，并负责对整改后的系统进行复测。
5.	商用密码应用安全性评估（含商用密码方案评审）	须配合系统测试方开展商用密码应用安全性评估工作，提供必要的设备、软件清单，并负责完成问题整改。 须提供计量自动化系统商用密码应用方案采集监控域分布式平台建设部分供系统测试方审查并负责完成问题整改。	负责开展商用密码应用安全性评估工作，提供必要的测试结果、整改意见，并负责对整改后的系统进行复测。
6.	电力监控系统安全防护评估	须配合系统测试方开展电力监控系统安全防护评估工作，提供必要的设备、软件清单，并负责完成问题整改。	负责开展电力监控系统安全防护评估工作，提供必要的测试结果、整改意见，并负责对整改后的系统进行复测。
7.	渗透测试	须配合系统测试方开展渗透测试工作，提供必要的设备、软件清单，并负责完成问题整改。	须配合系统测试方开展渗透测试工作，提供必要的设备、软件清单，并负责完成问题整改

3.4 中标方技术项目建设保障要求

中标方有责任为平台业务正常上线提供项目建设保障要求，本项目采购计量自动化系统分布式平台硬件设备及软件组件为最低功能及性能要求，如有未列出的，且是计量

主站系统及计量自动化系统分布式平台正常运行所必须依赖的硬件设备及软件组件，如服务器、交换机、安全设备及配套的光模块、内存、硬盘、Raid 卡和软件组件等，投标方需在投标时说明，否则视为投标方默认提供，由投标方无条件免费提供。

4 双方工作安排

4.1 贵州电网公司职责

(1) 审查合同生效后中标方提供的技术文件和图纸，审议并确认项目进度、技术联络会程序、培训内容和计划、验收测试大纲和计划等。

(2) 提供相关系统支撑资料。

(3) 提供必要的通信通道。

(4) 提供满足合同设备运行条件的现场运行环境。

(5) 提出现场的硬件布置要求。

(6) 参加技术联络会。

(7) 参加系统培训。

(8) 参与系统建设工作（包括模型创建、图形画面及各类统计报表模板的制作等）。

(9) 其它双方约定的贵州电网公司职责。

4.2 投标方职责

投标方职责包括但不限于：

(1) 按照招标技术要求，负责设计、开发、生产、集成一套符合要求的系统，并提供相应的技术服务，保证完全符合技术规范的要求。

(2) 提供系统运行所需的各类支撑软件（不包括已经明确说明另外采购的软件）。

(3) 负责软硬件设备的安装调试、IP 划分、网络及安防策略配置、数据录入或导入等工作。

(4) 配合贵州电网公司、监理方对第三方设备/软件/施工等进行测试验收。

(5) 负责所有的合同谈判和技术联络会。

(6) 负责软硬件设备到货验收及问题整改，配合“贵州电网公司计量自动化系统 3.0 建设”项目整体的系统试运行、现场验收（SAT）、竣工验收等验收工作，并负责整理并提供本项目相应验收所需资料。

(7) 提供系统测试方法和测试数据。

(8) 负责完成与贵州电网公司所有相关系统集成的配合工作(包括局域网互联、远程通信、与现有其它系统的接口等)。

(9) 负责供货范围内设备的投运、验收测试、试运行和保修期内的故障排除。

(10) 负责供货范围内所有设备的包装运输、临时仓储（含二次运输），并搬运至贵州电网公司指定的位置。

(11) 负责按照要求提供全面的技术培训，负责培训贵州电网公司的工程师及使用人员，协助贵州电网公司工程师和使用人员掌握相关职业证书的技术技能，获得证书不少于 7 人；负责培训在中标方平台上进行开发的第三方厂家工程师，包括但不限于软件培训、系统操作、维护培训和应用软件开发培训等；并负责提供培训环境，及由此产生的交通、食宿、会务等费用。

(12) 提供开发时原厂人员的技术支持，以及开发用的技术资料等。

(13) 在质保期内提供免费保修服务，并在系统使用期内提供技术支持。

(14) 及时向贵州电网公司通告有关软件的升级和更新，在质保期内应免费提供并负责安装和调试。

(15) 针对本项目的投标产品，提供全套的技术资料和文件，并对其正确性负责。主要技术资料包括但不限于如下内容：实施方案编制（包括施工图草图）、竣工资料、设备技术说明书和使用说明书、软件的技术说明书和使用说明书、产品型式试验和常规试验数据及试验报告、试验和验收标准、质量保证书和其它必需的资料。

(16) 负责整个系统的集成，负责硬件安装调试，负责软件功能的现场安装、生成和调试，负责按照贵州电网公司的要求创建系统模型、图形、报表，进行参数的录入及原系统历史数据的导入等。投标方技术专家在系统功能调试和试运行期间，为贵州电网公司及施工方提供良好的建议和指导。

(17) 有责任对贵州电网公司所提供的电网技术参数资料以及有关资料进行保密。

(18) 投标方提供的系统应当是一个开放的系统，投标方应配合贵州电网公司实现后续的系统功能建设，贵州电网公司或经贵州电网公司同意的任何第三方均可以在投标方提供的系统基础上进行二次开发、新系统集成和第三方软件接入，投标方应提供积极的响应，并完成相应的配合工作，不得以任何理由加以限制或制造障碍。

(19) 其它双方约定的投标方职责。

5 采购范围

5.1 供货总体要求

5.1.1 软硬件安全总体要求

(1) 对于核心网络设备、高性能计算机和服务器、大容量存储设备、大型数据库和应用软件、网络安全设备、云计算服务，以及其他对关键信息基础设施安全有重要影响的网络产品和服务，中标方必须严格落实国家互联网信息办公室等联合制定《网络安全审查办法》，认真执行《网络安全审查工作指引》《进一步加强采购管理有关要求》、《公司网络安全审查工作规范》等规定及有关要求，切实保障关键信息基础设施安全。

(2) 根据国家《网络安全审查办法》要求，经贵州电网有限责任公司预判为需要向国家网络安全审查办公室申报网络安全审查的产品或服务，中标候选人/中标人有义务配合网络安全审查工作，所需申报材料应在接到招标人通知的 3 个工作日内提供，并不得利用提供产品和服务的便利条件非法获取用户数据、非法控制和操纵用户设备，无正当理由不得中断产品供应或必要的技术支持服务，产品和服务通过网络安全审查后方可确定中标人，未通过网络安全审查的取消中标资格。凡参与本次投标的投标方，视作承诺上述事项，中标候选人/中标人产品和服务因没有通过网络安全审查而造成的损失，自行承担相关责任与后果；中标候选人/中标人因未履行网络安全审查义务（包括不配合审查、故意隐瞒、提供虚假申报材料等）而造成招标人直接或间接损失的，招标人保留追究责任权利。

(3) 本次供货的软硬件设备均应满足安全自主可控要求，提供的所有技术和组件都必须具备自主知识产权，符合国家相关政策标准，避免潜在的产权纠纷，原则上不使用开源软件。

(4) **根据国家发改委 2024 年第 27 号令《电力监控系统安全防护规定》要求，电力监控系统优先选用安全可信的产品和服务。不得选用存在已知安全缺陷、漏洞等风险但未采取有效补救措施的产品和服务。提供的产品和服务未设置恶意程序、不存在已知安全缺陷和漏洞，并在产品和服务的全生命周期内负责；当产品和服务存在安全缺陷、漏洞等风险时，立即采取补救措施，并及时告知运营者；当存在重大漏洞隐患时，及时向国家能源局及其派出机构报告。**

(5) 本次供货的软硬件产品均需保障产品本体安全，服务器（CPU、SSD、DRAM、BMC、网卡、电源六类芯片）、路由器、交换机、防火墙（CPU、DRAM、FLASH、

交换/转发芯片四类芯片）、电力专用网安设备四类芯片（CPU、DRAM、FLASH、安全芯片四类芯片）、数据库（分布式、集中式）、操作系统（桌面版、服务器版）等核心产品应通过国家权威机构安全可靠测评并提供对应产品的《安全自主可控承诺书》、《整机承诺函》、《芯片供应商承诺函》、《核心芯片应用统计表》等材料，并承诺在“贵州电网公司计量自动化系统 3.0 建设”项目竣工验收前提供对应产品的证书或认证，承诺格式详见技术建议书编制要求。产品本身所依赖的数据库（分布式、集中式）、操作系统（桌面版、服务器版）等产品也均应通过国家权威机构安全可靠测评，并包含在产品的供货范围中。所有产品中不得包含镁光（Micron）产品及镁光（Micron）芯片。若提供的产品不满足相关本体安全要求，中标方需负责免费更换相关的芯片、设备、软件等产品。服务器、数据库、操作系统应满足《附件 3：政府采购需求标准》中对应投标产品形态的技术参数要求，若《附件 3：政府采购需求标准》与正文产品技术参数要求有不一致，以利于贵州电网公司的最高技术要求为准。

(6) 本次供货的列入《网络关键设备和网络安全专用产品目录》的网络安全专用产品应当具备以下任意条件之一：

①应按照《信息安全技术网络安全专用产品安全技术要求》等相关国家标准的强制性要求，由具备资格的机构安全认证合格或者安全检测符合要求。需提供产品具有安全认证合格证明材料或者符合《信息安全技术 网络安全专用产品安全技术要求》强制要求的证明材料，同时需证明相关材料的提供机构在《承担网络关键设备和网络安全专用产品安全认证和安全检测任务机构名录》之内。

②具备有效期内的国家安全产品销售许可，提供国家公安部《计算机信息系统安全专用产品销售许可证》。

(7) 本次供货的数据库、数据计算组件、对象存储需提供配套的专业开发及运维工具，所有操作工具、客户端和软硬件设备，都应满足安全自主可控要求，兼容安全自主可控环境，可部署在安全操作系统上，应适配本次供货的数据库审计及日志审计设备，可审计到工具发出的所有操作及指令，应兼容并适配本次供货的国密堡垒机设备。

(8) 投标方应提供云平台产品自身依赖的组件，保障平台的正常运行，云平台自身应满足等级保护第三级测评（包括通用第三级安全要求及云计算扩展第三级安全要求）及商用密码安全性评估第三级测评要求。应在软硬件技术要求基础上，必要时应增配提供云平台产品自身达到等级保护第三级测评（包括通用第三级安全要求及云计算扩展第

三级安全要求）85 分及以上所需的软硬件设备，并包含在投标报价中。必要时应增配提供云平台产品自身达到商用密码安全性评估第三级测评合格分及以上且密码应用无高风险所需的软硬件设备，并包含在投标报价中。

(9) 投标方所提供的计量自动化系统分布式平台、虚拟化技术平台及 I 区基础环境的软硬件设备本体自身应满足商用密码应用安全性评估测评三级测评的要求，应兼容所投密码服务管理平台，支持调用密码服务管理平台的服务，中标方在实施过程中应采取技术措施以保障平台达到商用密码应用安全性评估测评第三级测评合格分及以上且密码应用无高风险；应满足等级保护第三级测评 85 分及以上的要求，必要时应增配软硬件达到等级保护第三级测评的要求，并包含在投标报价中。

(10) 投标方所提供的密码服务管理平台及密码应用方案应充分考虑异常处理机制，密码服务管理平台自身出现问题时，对于计量自动化主站系统的核心业务，应优先保障业务系统的正常运行。

(11) 本次供货的计量自动化系统分布式平台、虚拟化技术平台相关组件，在部署第三方安全代理组件或引流时，其功能、性能及稳定性应不受影响，供应方应配合第三方完成相关的实施工作，相关费用全部包含在本次投标报价中。

以上要求在“贵州电网公司计量自动化系统 3.0 建设”项目竣工验收之前要满足南网公司及贵州电网相关最新安全范文和审查的技术要求，并负责按照最新要求进行整改，相关整改涉及到的软件授权、硬件增配或改造、配套材料和施工等均含在本次项目投标报价中。

5.1.2 软硬件供货配置基本要求

本技术规范书的方案配置为最低要求，投标方提供的报价清单，应包括本技术规范书所要求的全部软硬件设备、材料和服务，投标方根据其产品特点认为应增加的软件（含授权）及硬件设备、材料和服务，必须包含在本次报价清单中。如有本技术规范书未列出的软硬件，投标方可予以补充，并对补充的内容或技术的必要性进行具体的论述。在实施过程中，为了满足本技术规范书要求，中标方未配置的软件（含授权）及硬件设备、材料和服务必须免费提供并保证符合质保要求。以上发生的费用均包含在报价之内。

本项目技术参数约定中，“支持”含义为，中标方应为本项目提供产品所依赖的软件组件、硬件配件等，保障设备的正常运行，保障软硬件技术参数条款中“支持”对应条目的执行，并包含在投标报价中。

5.1.2.1 硬件供货配置基本要求

(1) 投标方应结合本项目整体建设需求，根据投标技术方案和本次所投软硬件产品实际需求，提供能够实现系统整体运行指标的服务器数量和配置，满足系统稳定运行和性能相关指标要求。

(2) 本次供货的块存储（分布式存储）、对象存储若采用非三副本技术，则供货的分布式存储设备、对象存储服务器等硬件资源均应按照三副本技术计算的设备数量和硬件配置作为最低供货要求，且需要同时提供配套的满足投标技术路线需求的软件授权，包含在本次项目投标报价中（投标方应同时给出可用容量的计算公式等相关信息）。

(3) 各个安全区域内的数据库、中间件均要求以集群形态进行部署，本次投标需包含对应的集群软件，并包含在投标报价中。若不能以集群形态部署，需要在投标时进行说明，并提供更优的解决方案。

(4) 硬件设备的选择应遵循以下的基本要求：

1．关键设备采用冗余配置方式，单台设备故障不能相互影响；

2．原则上所有设备（包括服务器、存储设备、网络交换机、防火墙、密码机等）至少配置两路独立供电的电源，任意一路电源故障设备功能应不受影响；

3．硬件设备要选择通用标准且互换性高的产品，具有良好的开放以及低维护成本；

4．系统硬件设备的生命周期要求可以运行 8-10 年不需要进行大的升级改造；

5．硬件配置必须符合系统体系原理，满足系统性能和功能要求，并且符合实时性、安全性和可靠性原则；

6．充分考虑硬件资源复用；

7．充分考虑各业务模块的能力开放，支撑主站各业务功能模块采用微服务的方式进行开发及部署。

8．服务器的单根内存型号配置应该≥64GB。

9．同一类软件组件下涉及到的服务器配件应保持规格一致，不应出现多个规格、品牌。

5.1.2.2 软件供货配置基本要求

(1) 本次供货软件功能必须的组件，投标方应根据软件产品特点优化配置软件功能组件并提供相关软件的授权。如果上述本次采购组件未列出的系统功能是平台正常运行所依赖的组件，则由投标方免费提供，含在本次报价中。

(2) 本次供货的所有计量自动化系统分布式平台组件，版本应为云计算平台原厂的主力商用版本，该版本应解决了所有前序版本的遗留问题并且是从一线到研发全员主力长期保障的版本，避免频繁升级。且云计算平台的版本升级以及其组件升级，不应导致业务中断，不影响业务系统正常运行。且平台数据库及相关成套组件，应提供便捷的可视化工具，可视化工具应安全自主可控并兼容系统环境，提升开发及运维效率。

(3) 本次供货的软件模块应符合开放性、标准化的要求，方便以后功能升级或扩充，保障后续项目顺利实施。

(4) 软件授权为参考本项目配置服务器节点数（含单台服务器的 CPU、内存、存储等配置信息）提出的授权要求，若厂商授权模式与授权单位要求不符合，需要厂商进行说明并给出换算公式，折算为本技术规范书提出的授权单位形式要求，并满足授权数量要求，若不做说明均以本项目授权要求的单位形式为准。

(5) 为满足本平台后续扩容需求，云平台应支持 ARM、x86 等多种芯片架构服务器的混合部署功能，提供相关的方案说明并提供第三方测评报告等证明资料。

(6) 中标方应承诺：在整个系统运行生命周期内，贵州电网公司有权对平台软件组件应急扩容（扩容的软件组件授权数量不超过本次招标范围的 50%），中标方应配合贵州电网公司进行应急扩容工作，费用含在本次报价中。

(7) 在“贵州电网公司计量自动化系统 3.0 建设”项目竣工验收前，本次供货的软件授权可以按照中标的软件授权单价进行软件授权的无条件等价转换（即软件授权从一种软件组件调整到另外一个软件组件），转换时不应限定分布式平台类型、CPU 架构、组件类型等，含在本次项目的报价中。

(8) 本次采购中采集监控域软件授权具体约定如下：

1．软件授权均为永久授权，本项目采购的软件中的授权数量均指永久授权数量；

2．单位“套”：操作系统成套软件的套定为安装在一台物理机或一个虚拟机上的一套软件；其他软件授权套含义为本项目采购硬件内不限制安装的节点数、虚拟机数、客户端数、连接数等各类前置条件，即在本项目购置设备中安装和使用不做任何限制，软件授权同时包含平台侧和租户侧；软件授权同时涵盖“生产环境、开发测试环境”等不同环境配置相关授权；软件授权应支持不同 CPU 架构、不同的应用环境下的无缝迁移，费用包含在本次采购中。

3．单位“逻辑核”：逻辑核为不做资源共享物理核折算，一个 x86 架构物理核折算

为两个逻辑核。若 CPU 架构为 Arm 架构则授权数量需要对应 x86 给出，满足本次采购需要，若 Arm 没有逻辑核则按照物理核给出授权；当按照共享模式实施时，其共享模式下的软件授权应涵盖本次供货的所有硬件资源，不应进行任何授权限制。

4．单位“物理机台”：软件按照物理服务器形态安装或使用，涵盖范围为物理设备的授权单位，即授权数量为物理服务器的节点数，不限制服务器内部配置的 CPU、内存等各类配套资源；

5．单位“存储容量”：存储容量为给到用户最终使用的可用存储容量，非物理磁盘的裸容量，可用存储容量计算时应包括了磁盘格式化折损、副本技术、安全水位线等各类损耗，为最终业务方可以使用的容量；

6．软件组件依赖授权：本次采购的软件授权为独立的授权要求，若该组件依赖平台其他的组件授权则认为包含在采购的软件组件授权中。例如：分布式消息队列的授权依赖大数据平台的授权或云平台底座的授权，那么分布式消息队列的授权已经包含了大数据平台或云平台底座的授权，不得收取对应的依赖的软件组件授权费用；

7．硬件依赖授权：本次采购授权根据采购清单中服务器的 CPU 核数、存储等资源进行的测算，若供货平台厂家提供的硬件配置比采购清单要求的数量和参数高，那么硬件对应的软件组件授权也包含在项目的软件授权要求中，不得收取对应的软件组件授权费用，即本次供货的硬件均应包括对应的软件授权；包括但不限于如下情况：（1）投标的产品数量、配置等比招标的最低要求多，则本次投标包含对应的软件授权；（2）本次招标中可用存储容量对应的软件授权应包含全部容量授权含安全水位线以上的容量授权，例如：存储裸容量为 100TB，可用容量计算公式若只有安全水位线 0.85，那么可用容量为 85TB，此种情况下提供的硬件存储容量不少于 100TB，软件授权也应不少于 100TB；

若投标方的软件授权单位及形式与本技术规范书不符，均以本技术规范书约定为准，并提供软件授权转换说明，并转换为本技术规范书约定的软件授权形式进行供货。

5.2 硬件需求清单

5.2.1 不在本标的采购的甲供设备

态势感知系统采集装置与本项目相关，由建设单位提供，中标单位需要把本标的供货的软硬件设备接入到态势感知系统采集装置中。

序号	安全分区	设备	单位	数量
1.	安全III区	态势感知系统采集装置	台	2

序号	安全分区	设备	单位	数量
2.	安全Ⅱ区	态势感知系统采集装置	台	2
3.	安全接入区	态势感知系统采集装置	台	2
4.	安全Ⅰ区	态势感知系统采集装置	台	2

5.2.2 安全III区

5.2.2.1 服务器需求清单

结合系统功能业务应用、计量自动化系统分布式平台实现方案和技术路线，本次项目建设所需计算、存储等设备及对应设备配置清单如下所示。

下表服务器清单中的数量、配置参数等均为参考配置，投标方提供的服务器配置如服务器数量、CPU、内存、存储等均应大于等于下面清单中的参数，否则视为负偏差。

本次供货的分布式存储系统，均应优于授权清单，以及存储资源需求表中对应的存储容量需求。

表中数据库服务器的存储 SSD 类型应当配置 NVME SSD，NVME SSD 硬盘应当支持热插拔。事务型关系数据库必须以集群形式部署。

存储配置中，服务器本地存储配置为 0 的，允许配置本地硬盘替代对应的块存储（分布式存储）容量。

若数据离线计算组件未使用到数据离线计算服务器-分布式列存服务器，则需将对应资源调整至数据离线计算服务器-1 中。

分布式平台底座服务器 25 台包含了安全三区平台全部技术组件所涉及到的管理节点服务器。投标单位可根据软件技术方案进行评估，若 25 台服务器大于总的各类管理节点需求量，可调整底座服务器到云服务器等其他组件服务器中，但服务器总的数量和配置不能低于技术规范要求。

分类	服务器名称	数量	CPU（X86）		CPU 物理核(ARM)		内存（GB）	系统盘（TB）	存储（TB）		服务器类型
			物理核	主频	物理核	主频			SSD	HDD	
底座服务器	分布式平台底座服务器	25	48	≥2.2GHZ	96	≥2.6GHZ	512	0.96	7.68	96	底座型服务器
计算服务器	云服务器	52	64	≥2.6GHZ	128	≥2.6GHZ	1024	0.96	3.84	0	性能Ⅰ型服务器
存储服务器	块存储服务器	12	48	≥2.2GHZ	64	≥2.6GHZ	512	0.96	46.08	0	存储Ⅰ型服务器
	对象存储服务	16	48	≥2.2GHZ	64	≥2.6GHZ	512	0.96	6.4	144	存储Ⅱ型服

分类	服务器名称	数量	CPU（X86）		CPU 物理核(ARM)		内存（GB）	系统盘（TB）	存储（TB）		服务器类型
			物理核	主频	物理核	主频			SSD	HDD	
	器										务器
	日志服务器	6	48	≥2.2GHZ	64	≥2.6GHZ	512	0.96	6.4	144	存储Ⅱ型服务器
网络服务器	网络服务器	8	64	≥2.6GHZ	128	≥2.6GHZ	512	0.96	0	0	通用型服务器
数据库服务器	事务型关系数据库服务器	7	64	≥2.6GHZ	128	≥2.6GHZ	1024	0.96	46.08	0	数据库型服务器
	分析型数据库服务器	98	64	≥2.6GHZ	128	≥2.6GHZ	1024	0.96	46.08	0	数据库型服务器
	内存数据库服务器	10	64	≥2.6GHZ	128	≥2.6GHZ	1024	0.96	15.36	0	性能Ⅱ型服务器
	数据传输服务服务器	3	64	≥2.6GHZ	128	≥2.6GHZ	512	0.96	0	0	通用型服务器
数据计算组件服务器	实时计算服务器	25	48	≥2.2GHZ	64	≥2.6GHZ	512	0.96	7.68	144	大数据型服务器
	分布式消息队列服务器	10	48	≥2.2GHZ	64	≥2.6GHZ	512	0.96	7.68	144	大数据型服务器
	离线计算服务器	22	48	≥2.2GHZ	64	≥2.6GHZ	512	0.96	7.68	144	大数据型服务器
	数据开发组件服务器	6	64	≥2.6GHZ	128	≥2.6GHZ	512	0.96	0	0	通用型服务器
中间件服务器	中间件服务器	4	64	≥2.6GHZ	128	≥2.6GHZ	512	0.96	0	0	通用型服务器
能力开放服务器	能力开放组件服务器	3	64	≥2.6GHZ	128	≥2.6GHZ	512	0.96	0	0	通用型服务器
安全服务器	安全组件服务器	10	64	≥2.6GHZ	128	≥2.6GHZ	512	0.96	0	0	通用型服务器
	总计	317									

注：HDD 指 SATA/SAS HDD

5.2.2.2 网络设备需求清单

以下章节所示网络设备需求清单，投标方应保证所供设备配置能够满足技术规范书中数量、功能、性能和容量等要求。

本项目涉及的网络设备，供货方均应随主设备配置完整、满配的光模块，具体数量及技术选型以贵州电网公司实际需求为准。

如以下网络设备实际组网运行后的功性能、兼容性、数量等不满足云计算平台组网的性能、功能要求时，则中标方应免费提供网络设备，以支撑业务的正常运行，对应的

设备及配套的配件、材料和施工均含在本次投标报价中。

5.2.2.2.1 云网络设备需求清单

下表所示为云网络设备需求清单，投标方应保证所供配置能够满足技术规范书对于需求数量、功能、性能等要求。

序号	设备	单位	数量
1.	核心交换机	台	2
2.	接入交换机-25GE	台	16
3.	带外管理交换机	台	10
4.	接入交换机（数据库）-25GE	台	6

5.2.2.2.2 配套网络设备需求清单

下表所示为配套网络设备需求清单，投标方应保证所供配置能够满足技术规范书对于需求数量、功能、性能等要求。

序号	设备	单位	数量
1.	汇聚交换机	台	2
2.	千兆交换机（开发、测试）	台	4
3.	千兆交换机（运维）	台	2

5.2.2.3 安全设备需求清单

下表所示为安全设备需求清单，投标方应保证所供配置能够满足技术规范书对于需求数量、功能、性能等要求。

序号	设备	单位	数量
1.	费控密码机	台	4
2.	万兆正向隔离装置	台	4
3.	万兆反向隔离装置	台	3
4.	边界防火墙	台	4
5.	运维区防火墙	台	2
6.	入侵防御设备	台	1
7.	网络终端接入核查设备	台	1
8.	堡垒机	台	2
9.	云出口防火墙	台	4
10.	持续威胁检测与溯源系统（APT）	台	1
11.	安全 U 盘	个	2
12.	杀毒 U 盘	个	2
13.	国密服务器密码机	台	4

5.2.2.4 配套设备需求清单

下表所示为配套设备需求清单，投标方应保证所供配置能够满足技术规范书对于需求数量、功能、性能等要求。

序号	设备	单位	数量	备注
1.	卫星时钟	台	2	
2.	瘦终端	台	150	与云平台云桌面服务兼容
3.	远程运维终端	台	20	远程运维用途

5.2.3 安全Ⅱ区、安全接入区

采集业务在安全 II 区、安全接入区采用基于容器的方式进行部署，需在贵州采集监控域机房配套部署虚拟化技术平台。

结合系统功能业务应用、虚拟化技术平台实现方案和技术路线，本次建设所需计算、存储设备及对应设备配置清单如下。

5.2.3.1 服务器需求清单

下表所示为服务器需求清单，投标方应保证所供配置能够满足技术规范书对于需求数量、功能、性能、容量等要求。

服务器主频均要求≥2.2GHZ，系统盘要求 RAID1，数据盘要求 RAID5。

(1) 安全Ⅱ区

服务器名称	数量	CPU 物理核（X86）	CPU 物理核（ARM）	内存（GB）	系统盘	存储（TB）		服务器类型
						SSD	HDD	
计算节点（前置接入、后置处理、密码接口服务）	22	48	96	256	0.96	0	8	非 III 区服务器(通用型)
管控节点	4	48	96	256	0.96	0	8	非 III 区服务器(通用型)
安全节点	3	48	96	256	0.96	0	48	非 III 区服务器(容量型)

注：HDD 指 SATA/SAS HDD

(2) 安全接入区

服务器名称	数量	CPU物理核（X86）	CPU物理核（ARM）	内存（GB）	系统盘	存储（TB）		服务器类型
						SSD	HDD	
计算节点（前置接入、后置处理、密码接口服务）	28	48	96	256	0.96	0	8	非III区服务器(通用型)
管控节点	4	48	96	256	0.96	0	8	非III区服务器(通用型)
安全节点	3	48	96	256	0.96	0	48	非III区服务器(容量型)

注：HDD 指 SATA/SAS HDD

说明：表格中设备资源数量为最低配置要求。配置清单仅作参考，实际计算、存储资源配置以技术验证选型后配置为准。

5.2.3.2 网络设备需求清单

以下所示网络设备需求清单，投标方应保证所供设备配置能够满足技术规范书中数量、功能、性能和容量等要求。

本项目涉及的网络设备，供货方均应随主设备配置完整、满配的光模块，具体数量及技术选型以贵州电网公司实际需求为准。

如以下网络设备实际组网运行后的功性能、兼容性、数量等不满足虚拟化技术平台组网的性能、功能要求时，则中标方应免费提供网络设备，以支撑业务的正常运行，对应的设备及配套的配件、材料和施工均含在本次投标报价中。

序号	安全区域	设备类别	单位	数量
1.	安全II区	万兆采集交换机	台	2
2.		万兆接入交换机	台	2
3.		千兆管理交换机	台	2
1.	安全接入区	万兆采集交换机	台	2
2.		万兆接入交换机	台	4
3.		千兆管理交换机	台	2
4.		北斗通信管理机	台	2
5.		负载均衡器	台	2

注：配置仅作参考，实际网络、安全资源配置以技术验证选型后配置为准。

5.2.3.3 安全设备需求清单

下表所示为安全设备需求清单，投标方应保证所供配置能够满足技术规范书对于需求数量、功能、性能等要求。

序号	安全区域	设备类别	单位	数量
1.	安全 II 区	费控密码机	台	2
2.		千兆纵向加密认证网关（调度数据 A 网、调度数据 B 网）	台	4
3.		边界防火墙（接入）	台	2
4.		边界防火墙	台	2
5.		运维区防火墙	台	2
6.		入侵防御设备	台	1
7.		网络终端接入核查设备	台	1
8.		堡垒机	台	2
9.		数据库审计	台	1
10.		日志审计	台	1
11.		漏洞扫描	台	1
12.		持续威胁检测与溯源系统（APT）	台	1
13.		安全 U 盘	个	2
14.		杀毒 U 盘	个	2
15.		国密服务器密码机	台	2
1.	安全接入区	万兆正向隔离装置	台	3
2.		万兆反向隔离装置	台	3
3.		边界防火墙（接入）	台	2
4.		运维区防火墙	台	2
5.		入侵防御设备	台	1
6.		网络终端接入核查设备	台	1
7.		堡垒机	台	2
8.		计量通信认证网关	台	1
9.		数据库审计	台	1
10.		日志审计	台	1
11.		漏洞扫描	台	1
12.		持续威胁检测与溯源系统（APT）	台	1
13.		安全 U 盘	个	2
14.		杀毒 U 盘	个	2
15.		国密服务器密码机	台	2

5.2.3.4 配套设备需求清单

下表所示为配套设备需求清单，投标方应保证所供配置能够满足技术规范书对于需求数量、功能、性能等要求。

序号	部署区域	设备	单位	数量
1.	安全Ⅱ区	卫星时钟	台	2
2.		运维终端	台	2
1.	安全接入区	卫星时钟	台	2
2.		运维终端	台	2

5.2.4 安全Ⅰ区

5.2.4.1 服务器需求清单

结合系统功能业务应用实现方案和技术路线，本次安全Ⅰ区建设所需服务器配置清单如下所示。

服务器主频均要求≥2.2GHZ，系统盘要求 RAID1，数据盘要求 RAID5。

序号	服务器名称	数量	单位	CPU 物理核（X86）	CPU 物理核（ARM）	内存(GB)	系统盘	存储（TB）		服务器类型
								SSD	HDD	
1.	I 区跨区传输服务器	4	台	48	96	256	0.96	0	8	非 III 区服务器（通用型）
2.	I 区负控服务器	4	台	48	96	256	0.96	0	8	非 III 区服务器（通用型）
3.	密码接口服务器	2	台	48	96	256	0.96	0	8	非 III 区服务器（通用型）
4.	安全节点	2	台	48	96	256	0.96	0	48	非 III 区服务器（容量型）

注：HDD 指 SATA/SAS HDD

5.2.4.2 网络设备需求清单

以下所示网络设备需求清单，投标方应保证所供设备配置能够满足技术规范书中数量、功能、性能和容量等要求。

本项目涉及的网络设备，供货方均应随主设备配置完整、满配的光模块，具体数量及技术选型以贵州电网公司实际需求为准。

序号	设备名称	单位	数量
1	万兆接入交换机	台	2
2	千兆管理交换机	台	2

5.2.4.3 安全设备需求清单

下表所示为安全设备需求清单，投标方应保证所供配置能够满足技术规范书对于需

求数量、功能、性能等要求。

序号	部署区域	设备	单位	数量
1.	安全Ⅰ区	费控密码机	台	6
2.		入侵防御设备	台	1
3.		运维区防火墙	台	2
4.		蜜罐设备	台	1
5.		网络终端接入核查设备	台	1
6.		堡垒机设备	台	2
7.		数据库审计	台	1
8.		日志审计	台	1
9.		漏洞扫描	台	1
10.		持续威胁检测与溯源系统（APT）	台	1
11.		安全 U 盘	个	2
12.		杀毒 U 盘	个	2
13.		国密服务器密码机	台	2

5.2.4.4 配套设备需求清单

下表所示为配套设备需求清单，投标方应保证所供配置能够满足技术规范书对于需求数量、功能、性能等要求。

序号	部署区域	设备	单位	数量
1.	安全Ⅰ区	卫星时钟	台	2
2.		运维终端	台	2

5.3 软件需求清单

以下章节所示为软件需求清单，投标方应保证所供软件配置能够满足技术规范书中数量、功能、性能和容量等要求。平台软件版本必须为供应商最新的稳定版本。

5.3.1 安全Ⅲ区

5.3.1.1 计量自动化系统分布式平台软件功能需求清单

下表所示为计量自动化系统分布式平台软件功能需求清单，投标方应保证所供配置能够满足技术规范书对于需求数量、功能、性能和容量等要求。

序号	组件类型	组件名称	配置要求（其中容量为可用容量）	单位	说明
1.	云平台底座	分布式云操作系统	1	套	分布式云操作系统是一种新型的云计算操作系统，将云

序号	组件类型	组件名称	配置要求（其中容量为可用容量）	单位	说明
					计算的服务和管理能力延伸到了分布式的环境中，实现了对分布式云资源的统一管理和调度。 应满足本次投标安全 III 区的全部服务器部署要求。
2.		运营管理	317	物理机台	主要面向云资源的使用者及管理员，提供完整云平台运营能力。 应满足本次投标安全 III 区的服务器及存储设备规模。
3.		运维平台	317	物理机台	运维平台作为云管理平台的核心功能组件，提供集中化的云平台运维能力。 应满足本次投标安全 III 区的服务器及存储设备规模。
4.	弹性计算	云服务器	6136	逻辑核	业务可用数量。 云服务器是一个虚拟的计算环境，包含 CPU、内存等最基础的计算组件。
5.		容器服务	6136	逻辑核	业务可用数量。 容器服务是一种高性能可伸缩的容器管理服务。 提供的软件授权应包含依赖的软件组件授权，例如：若容器服务依赖云服务器等软件授权，则应当对应容器服务授权数量，提供对等的云服务器授权及其他容器服务部署必须依赖的软件授权。
6.		容器镜像服务	1	套	容器镜像服务标准版，支持容器镜像的安全托管及高效分发。
7.		弹性伸缩	1	套	弹性伸缩服务控制伸缩组中云服务器的数量，进行扩容和减容操作
8.		资源编排	1	套	资源编排服务的编排引擎将根据模板自动完成所有资源的创建和配置，实现自动化部署及运维。
9.	存储服	块存储	141	TB	业务可用数量。

序号	组件类型	组件名称	配置要求（其中容量为可用容量）	单位	说明
	务				块存储服务是一种基于分布式架构的、可弹性扩展的虚拟块存储设备
10.		对象存储服务	587.52	TB	业务可用数量。 对象存储将数据文件以对象形式上传到存储空间中，提供键值对形式的存储服务
11.		虚拟机备份服务	1	套	虚拟机备份
12.	网络	负载均衡服务	1	套	负载均衡是将访问流量根据转发策略分发到后端多台云服务器的流量分发控制服务
13.		专有网络	1	套	云上私有网络
14.		NAT 网关	1	套	提供 NAT 代理（SNAT 和 DNAT）功能
15.		VPN 网关	1	套	基于外网（综合数据网等）的网络连接服务
16.		专有云 DNS	1	套	企业内网环境（专有云网络）提供域名解析服务
17.	云桌面	云桌面	200	用户	电脑的主机、CPU、硬盘等硬件设施都集中在云端； 提供的软件授权应包含依赖的软件组件授权：例如：若云桌面依赖云服务器等软件授权，则应当对应云桌面授权数量，提供云服务器授权及其他云桌面部署必须依赖的软件授权。
18.	数据库服务	事务型关系数据库（TP 库）	82.25	TB	业务可用数量。 关系型数据库，提供高吞吐强一致性事务处理能力、高可用能力、大数据高性能查询能力。
19.		分析型数据库（AP 库）	1151.5	TB	业务可用数量。 提供交互式分析型数据库服务，支持高并发和低延时地分析处理 PB 级数据。
20.		内存数据库	3727.5	GB	兼容 Redis 协议标准、提供可靠的缓存数据库服务
21.		数据传输服务	1	套	提供了实时迁移、批量迁移、实时同步、数据订阅和实时灾备等多种功能。

序号	组件类型	组件名称	配置要求（其中容量为可用容量）	单位	说明
22.		数据库管理	1	套	面向 TP 库，AP 库，内存库的管理能力
23.		数据库备份	1	套	提供数据库备份能力
24.		数据库自治	1	套	面向 TP 库，AP 库，内存库的安全，运维能力
25.	中间件服务	企业级分布式应用服务	6136	逻辑核	业务可用数量。 应用托管和微服务管理的云原生 PaaS 平台
26.		消息队列	1	套	基于高可用分布式集群，提供消息订阅发布等功能
27.		应用实时监控	1	套	应用实时监控
28.		云服务总线	1	套	提供轻量化消息、数据、API、设备等集成能力，简化企业上云流程，支持云上云下、跨区域 集成
29.		日志服务	1	套	日志数据采集、消费以及查询分析，提升运维、运营效率，建立海量日志处理能力
30.		API 网关	1	套	提供完整的 API 托管服务，覆盖 API 全生命周期管理
31.	数据计算组件	实时计算	2400	逻辑核	包含实时数据采集和实时流处理能力 应至少提供同时满足处理性能和逻辑核要求的授权数量。
32.		离线计算	2112	逻辑核	提供分布式存储能力，支持 PB 级别数据处理与计算，支持结构化与非结构化数据存储 应至少提供同时满足存储可用容量和逻辑核要求的授权数量。
33.		分布式消息队列	58.8	TB	对流式数据的发布、订阅及分发功能，应至少提供同时满足存储可用容量和逻辑核要求的授权数量。
34.		数据开发组件	1	套	完成数据同步、开发、治理、服务、质量、安全等全套数据研发治理工作
35.		数据管理组	1	套	支持从业务、服务、集群和

序号	组件类型	组件名称	配置要求（其中容量为可用容量）	单位	说明
		件			主机等多个角度对大数据产品进行运维
36.	能力开放中心	协同研发平台	1	套	提供流水线管理、代码管理、制品管理等在内的开箱即用一站式服务
37.		BI 报表工具	1	套	提供海量数据实时在线分析服务
38.		数据可视化	1	套	完成数据接入与处理、可视化页面设计、数据分析、业务协同应用与分析支持等功能

5.3.1.2 安全软件功能需求清单

下表所示为安全软件功能需求清单，投标方应保证所供配置能够满足技术规范书对于需求数量、功能、性能和容量等要求。

序号	部署区域	分类	设备名称	单位	数量
1.	安全III区	边界安全	蜜罐系统	套	1
2.		平台侧	安全管理中心（平台侧）	套	1
3.			数据库审计（平台侧）	套	1
4.			日志审计（平台侧）	套	1
5.			主机安全（平台侧）	套	1
6.			漏洞扫描（平台侧）	套	1
7.			态势感知（平台侧）	套	1
8.			云堡垒机（平台侧）	套	1
9.			流量安全监控	套	1
10.		租户侧	安全管理中心（租户侧）	套	1
11.			数据库审计（租户侧）	套	1
12.			日志审计（租户侧）	套	1
13.			主机安全（租户侧）	套	1
14.			容器安全（租户侧）	套	1
15.			漏洞扫描（租户侧）	套	1
16.			云防火墙（租户侧）	套	1
17.			Web 应用防火墙（租户侧）	套	1
18.			态势感知（租户侧）	套	1
19.			云堡垒机（租户侧）	套	1

20.		密码安全	密码服务管理平台	套	1
21.		数据安全	数据脱敏	套	1
22.			数据水印	套	1

5.4 技术服务需求清单

序号	服务名称	服务要求	单位	数量
1.	集成实施技术服务	(1) 临时系统开发测试环境搭建 在中标后30天内在业主指定机房中完成开发测试环境搭建。中标方负责提供开发测试环境所需的资源，环境应采用风冷的制冷模式，并提供不少于生产环境的20%的可用资源，包括但不限于服务器、交换机、云平台基础组件、协同开发平台等全套的软硬件环境，软件版本应与生产环境保持一致。中标方应负责提供开发测试环境搭建所需的耗材，并负责实施和配置等工作，均由中标方自行评估并在投标文件明确罗列，开发环境应能保证主站应用功能建设开发厂家在系统上线前的正常开发、测试等工作。并且承诺后续可以免费迁移至计量检定中心机房。 此项工作所需的全部软硬件、配件、实施等建设内容应包含在本次投标报价中。 (2) 生产环境搭建 由中标方负责在计量检定中心机房搭建满足生产需要的开发、测试、生产等环境。具体环境划分以业主需求为准。 此项工作所需的全部软硬件、配件、实施等建设内容应包含在本次投标报价中。 (3) AI环境搭建 中标方负责搭建一套可以支撑业务人工智能应用的大模型环境，支持多模态、图像识别、语音识别、语义识别等，协助贵州电网公司开展大模型的业务应用训练等工作。 此项工作所需的相关建设和实施内容含在投标报价中。 (4) 硬件运输、卸车、搬运、保管服务 中标方应负责将所有供货设备运输到项目实施现场并卸车、搬运至安装机房，如因现场条件限制需在现场之外临时保管的，中标方应负责保管及二次运输，保障本项目采购的软硬件资	项	1

序号	服务名称	服务要求	单位	数量
		源在机房施工完成前的完整性、可用性，含在本次投标报价中。 (5) 硬件安装、接线、标识、调试服务（含材料） 中标方应负责本项目的硬件资源部署规划工作，提供施工图草图。 中标方应负责本项目硬件实施过程中，相关技术服务方案、实施方案、培训方案等技术方案的制订。 中标方应负责自动化机房至通信机房之间的尾纤接线工作（从自动化机房边界防火墙至通信机房路由器）。 中标方应负责机房内设备相关的网线、光纤的布线及标签标识等材料供应及现场实施：应负责所有供货设备的搬运、清洁、上架安装、接线（含配套电源线、网络跳线、光纤跳线、光纤模块等配套材料）、标签标识、设备配置、单体调试，确保设备稳定可靠运行，并应符合南方电网及招标人关于设备安装、接线、标签标识等方面的规范要求。 中标方需提供本项目 10GE 以上线缆的供货(包括但不限于 25GE、40GE 等），含在本次投标报价中。 配套机房及通信工程的综合布线不满足本项目部署要求的，需本项目中标方按照配套机房工程的建设标准要求，进行综合布线，含柜间和柜内的全部材料及实施工作。 (6) 软件安装调试服务 中标方应负责软件实施过程中，相关技术服务方案、实施方案、培训方案等技术方案的制订。 中标方应负责完成软件组件的安装部署、系统联调、功能性能测试、培训等。并配合完成必要的技术文档编制。 (7) 现场技术支持服务 中标方应提供技术支持、协助问题排查等技术服务。 中标方应负责组织开展技术联络、验收会议等项目相关工作。 中标方应在项目执行期间直到“贵州电网公司计量自动化系统 3.0 建设”项目竣工后 1 年内，提供至少 2 人每周 5x8 小时的计量自动化系统分布式平台原厂(提供社保)现场技术支持服务。 中标方应配合本项目主站应用功能建设开发厂家在平台的实施工作。 (8) 配合安全测试		

序号	服务名称	服务要求	单位	数量
		中标方需开展本项目相关的安全防护工作。 需配合第三方测试、等保测评及安全防护评估、商用密码应用安全性评估（含商用密码方案评审）、安全检测（含入网安全评测、源代码审计）、渗透测试、电力监控系统安全风险评估等安全评测，云边协同技术验证及建设质量评价研究服务，并负责完成问题整改，且整改方式不能采用临时解决方案，应为正式永久的解决方案。 需为本项目建设内容有针对性地提供计量自动化系统商用密码应用方案采集监控域分布式平台建设部分，保障方案通过测评单位评审。 在项目竣工前需提供第三方测评机构出具的源代码审查报告，交由测评机构对源代码审查报告的合理、合法、合规及安全性进行评估并要求通过评估，并负责完成问题整改。 (9) 满足本技术规范书“实施内容”章节内本项目工作内容要求、“项目实施要求”章节、“项目验收要求”章节、“售后服务要求”章节的实施、集成、技术服务、售后等等要求。 以上要求涉及的材料与服务的内容均应含在本次投标报价中。		

5.4.1.1 配套软件功能需求清单

下表所示为配套软件功能需求清单，投标方应保证所供配置能够满足技术规范书对于需求数量、功能、性能和容量等要求。

序号	分类	组件	单位	数量
1.	配套软件	服务器版安全操作系统	套	395
2.		桌面版安全操作系统	套	150
3.		国密浏览器	个	20

5.4.2 安全Ⅱ区、安全接入区

5.4.2.1 虚拟化技术平台软件功能需求清单

下表所示为平台软件功能需求清单，投标方应保证所供配置能够满足技术规范书对于需求数量、功能、性能和容量等要求。

序号	类别	软件名称	单位	数量
1.	安全接入区	基础设施服务（包含基础资源管理、应用服务、平台管理）	套	1
2.		容器服务	个（逻辑核）	2976
3.		企业级分布式应用服务	个（逻辑核）	1488
4.		分布式消息队列	套	1
5.		内存数据库	套	1
6.	安全Ⅱ区	基础设施服务（包含基础资源管理、应用服务、平台管理）	套	1
7.		容器服务	个（逻辑核）	2400
8.		企业级分布式应用服务	个（逻辑核）	1200
9.		分布式消息队列	套	1
10.		内存数据库	套	1

5.4.2.2 安全软件功能需求清单

下表所示为安全软件功能需求清单，投标方应保证所供配置能够满足技术规范书对于需求数量、功能、性能和容量等要求。

序号	部署区域	分类	设备名称	授权单位	数量
1.	安全接入区	网络安全	蜜罐系统	套	1
2.			主机安全	套	1
3.	安全Ⅱ区	网络安全	蜜罐系统	套	1

序号	部署区域	分类	设备名称	授权单位	数量
4.			主机安全	套	1
5.	安全接入区	密码安全	密码服务管理平台	套	1
6.	安全Ⅱ区	密码安全	密码服务管理平台	套	1

5.4.2.3 配套软件功能需求清单

下表所示为配套软件功能需求清单，投标方应保证所供配置能够满足技术规范书对于需求数量、功能、性能和容量等要求。

序号	部署区域	分类	组件	单位	数量
1.	安全接入区	配套软件	服务器版安全操作系统	套	35
2.			国密浏览器	套	20
3.	安全Ⅱ区	配套软件	服务器版安全操作系统	套	29
4.			国密浏览器	套	20

5.4.3 安全 I 区

下表所示为安全 I 区安全及配套软件功能需求清单，投标方应保证所供配置能够满足技术规范书对于需求数量、功能、性能和容量等要求。

序号	设备名称	单位	数量
1	主机安全	套	1
2	密码服务管理平台	套	1
3	服务器版安全操作系统	套	12

5.4.4 综合监管系统软件

下表所示为综合监管系统软件需求清单，投标方应保证所供配置能够满足技术规范书对于需求数量、功能和性能等要求。

序号	组件	单位	配置要求
1.	安全接入区态势感知中继系统	套	1
2.	安全Ⅱ区态势感知子站系统	套	1
3.	安全Ⅲ区态势感知子站系统	套	1

6 总体技术方案要求

计量自动化系统 3.0 建设属于“4321+”数字化转型中的数字电网建设，计量自动化系统 3.0 从量测装置、通信、平台及应用部署、数据流线及时性要求等方面均满足数字化

转型的指导原则要求，计量自动化系统 3.0 采用网、省两级级部署，采用一主两域、云边协同方式，划分为数据分析域和采集监控域，分别基于生产控制云主节点和边缘计算集群部署，具备部分 1 分钟的数据采集处理和存储要求。

为保障计量自动化基础核心功能安全稳定可靠运行，将海量数据挖掘分析等占用大量存储计算资源的功能剥离出来，计量自动化系统 3.0 按照采集监控域和数据分析域设计。采集监控域主要承载生产运行及实时数据共享等业务，数据分析域主要承载海量数据价值挖掘及非实时数据共享等业务。两个域软硬件独立部署，通过数据和应用交互实现计量自动化主站全部功能，并通过统一人机交互界面提供给公司各级人员访问使用。

采集监控域基于统一基座模式建设。基座主要对数据模型、算法规则、数据交互进行统一，实现基础的数据存储计算服务标准化，满足基础能力复用要求，并基于基座开展相关业务应用建设，部署在贵州计量检定中心机房。

数据分析域基于能力开放平台和交互共享平台建设。大数据域能力开放实现多源数据融合，提供基础能力、存储能力、计算能力和服务能力四个层次的能力开放，全面支撑各专业部门、基层单位开展电能量数据创新应用，部署在广州棠下数据中心。

本项目包括计量自动化系统分布式平台基础设施采购及安装调试实施。

6.1 建设要求

6.1.1 建设规模要求

本期系统建设拟满足贵州电网现有用户，并考虑从 2023 至 2028 年的用户增量情况，接入规模按厂站用户年增长率为 2%，公变用户年增长率为 3.5%，专变用户年增长率为 2%，低压集抄用户年增长率为 4%，光伏用户年增长率 10%来进行估算，至 2028 年主站系统接入测量点规模为 2348 万个。其中厂站、公/专变、光伏用户瞬时量、工况采集密度按照 1 分钟/次，表码作为累计量，密度需求不高，按照 15 分钟/次，低压重点用户（表码、瞬时量、工况）采集密度按照 15 分钟/次，低压普通用户（表码、工况）采集密度按照 1 小时/次。

6.1.2 计量场景技术要求

(1) 实时复杂数据分析查询

对应业务场景里面的抄表数据查询等业务对实时性要求比较高的业务，同时又需要关联多个档案进行复杂的数据查询，满足实时在线分析的时效性要求，具体来说，需实现复杂场景百亿级别的多表关联查询秒级返回的要求，响应时间应≤3 秒。

(2) 超大规模存储与计算

计量自动化系统 3.0 海量数据主要包括冻结类、曲线类、分钟级三种数据类型，在数据规模、重要程度、访问时效等方面需选择适用的数据库和存储策略、计算策略。因此需要完善而稳定的技术平台进行支撑，并为 PB 级的计算调度集群提供稳定保障。

(3) 完善的数据处理链路

计量自动化系统 3.0 应根据未来计量丰富的业务场景，满足多种实时和离线数据处理需求，比如以小时、日、周、月为单位的电量计算、针对某分析对象的电量计算、负荷叠加计算、电能质量分析等计算场景。

由于采用实时计算、离线计算，以及多种异构数据库技术，需要搭建数据处理链路，在不同技术组件之间进行数据的加工，过滤，清洗和计算处理，构建数据分层服务，实现整体处理能力超越 Oracle 单一数据库的处理能力的目标。

(4) 底座安全与底座容灾

计量自动化系统 3.0 基于云和数据计算组件来建设，技术的复杂度提升也带来了容灾和安全的复杂度，这些复杂度不应当由业务开发团队承担，应当由平台提供保障机制。

计量自动化系统 3.0 是一个复杂的技术体系，包含计算、网络、数据库、消息、中间件、存储、大数据等组件。首先每个组件都应该是高可靠设计，比如当某组件出现硬件故障时，组件应对故障进行屏蔽，防止局部故障波及整个系统的运行，其次平台应具备业务无感的平台级容灾能力，既要支持主备模式也要支持双活模式。主备模式下只有主机房的产品对外提供服务，出现故障时，需要通过容灾切换工具人工切换，切换时间通常为分钟级。

(5) 两域应用管理发布需求

本次计量自动化系统 3.0 需要采用微服务技术建设。微服务架构需要一套微服务平台对服务管理和发布进行支持，实现从需求管理，应用微服务开发，测试验证，生产发布到上线运维的一整套全生命周期的研运一体化管理体系。实现持续迭代运营需求。

(6) 全面安全自主可控需求

计量自动化系统 3.0 作为国家基础设施的重要部分，技术路线应当充分考虑安全自主可控趋势。依据《GB/T 36572-2018 电力监控系统网络安全防护导则》相关要求，构成计量 3.0 系统网络安全防护体系的各个模块应实现自身的安全，依次分为电力监控系统软件的安全、操作系统和基础软件的安全、计算机和网络设备及电力专用监控设备的

安全、核心处理器芯片的安全，包含依赖产品组件及部署环境，均应采用安全、可控、可靠的软硬件产品。

6.2 技术架构

计量自动化系统 3.0 的技术架构遵循公司数字化统一技术路线，依据计量自动化系统 3.0 相关规范的要求，按照“一主两域、云边协同”的总体设计思路，充分应用“云大物移智”等先进数字技术，架构将从集中式向分布式转变，支撑计量自动化系统 3.0 的功能建设。

计量自动化系统 3.0 的数据分析域依托调度云棠下延伸节点扩容；采集监控域建设在省侧边缘集群。技术架构如下图所示：

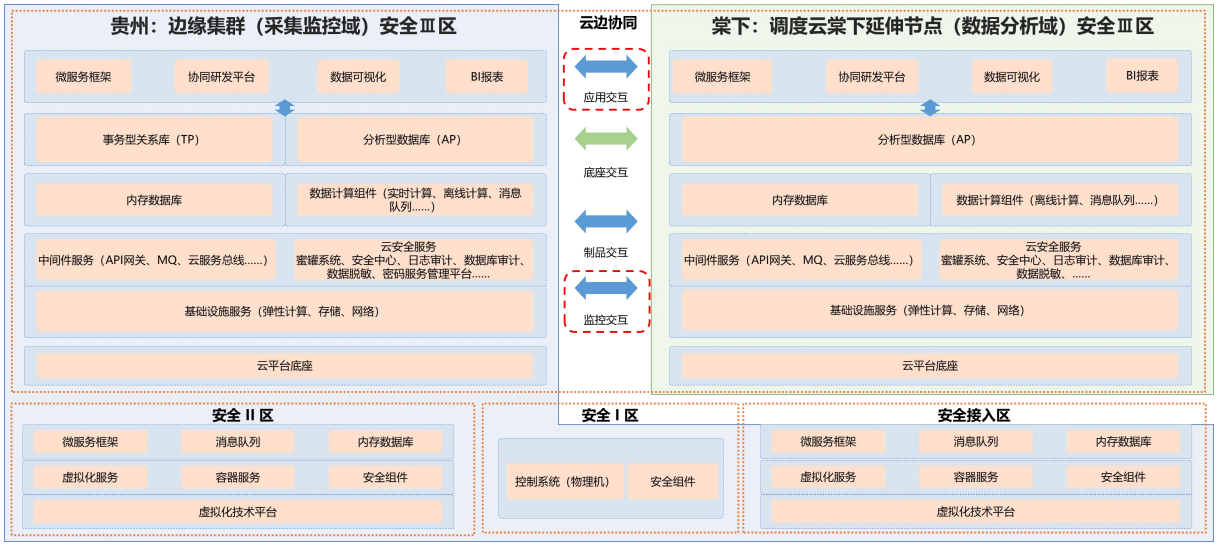

图 6-1 技术架构图

边缘集群采集监控域的技术架构内容如下：

(1) 安全接入区

安全接入区部署边缘集群，提供容器、微服务框架、分布式消息队列、内存数据库等组件；主站应用基于微服务框架开发，支持容器化部署，实现终端通讯接入、采集任务调度、报文转发等前置采集功能。

(2) 安全Ⅰ区

安全Ⅰ区部署控制子系统和跨区通讯服务。

(3) 安全Ⅱ区

安全Ⅱ区部署边缘集群，提供容器、微服务框架、分布式消息队列、内存数据库等组件；主站应用基于微服务框架开发，支持容器化部署，实现终端通讯接入、采集任务调度、报文转发等前置采集功能。同时为满足部分厂站侧专变用户远程费率设置，部署费控密码机及接口服务器提供加解密服务。

(4) 安全Ⅲ区

安全Ⅲ区部署边缘集群，提供虚拟化、容器、云平台管理等基础层服务，提供数据计算、数据存储、应用部署等平台层服务，满足采集监控域应用需求。

基础服务（IaaS）：提供虚拟化、容器、云平台管理等 IaaS 层服务。

数据计算组件：提供实时流式计算、批量离线计算组件；主站数据计算任务以计算组件的方式部署在大数据计算环境，计算任务统一调度、资源统一协调。

数据库服务：提供事务型关系数据库（TP 库）和分析型数据库（AP 库）；主站应用结合 TP 库与 AP 库，实现前端数据展现及应用支撑功能。

中间件服务：提供容器化部署、微服务运行框架等中间件服务；主站应用采用微服务架构实现前后端分离，后端业务微服务支持容器化部署。

业务支撑：主站充分应用基础服务、数据计算、数据库服务、中间件服务、数据同步服务能力，实现采集管理、运维管理、监测控制、基础应用、数据共享等业务支撑功能。

6.3 数据架构

6.3.1 整体架构

结合数据库的特点和特征，系统的典型业务场景下分析实时业务和非实时业务及大数据分析业务，通过技术路线分析前台应用主要使用的数据库包括事务型关系数据库（TP 库）和分析型数据库（AP 库）和大数据平台的存储；数据分析域的分析型数据库用于非实时业务的查询和分析，并支持与非关系数据库（历史库）实现数据同步。

采集监控域通过数据的拆分和业务应用拆分，采用事务型数据库、分析型数据库及大数据平台组合实现计量的绝大部分业务场景。

(1) 事务型关系数据库承担以下几个作用：

1．作为采集监控域档案源头，向内存数据库、分析型数据库、大数据平台、消息队列同步档案，支撑档案、日月冻结及事务业务处理等数据查询；

2．支撑高并发和小量数据查询的服务。

(2) 分析型数据库主要承担以下几个作用：

1．接受事务型关系数据库的档案数据同步；

2．支撑对实时性业务和非实时性业务查询；

3．支撑高并发和大量数据查询的服务，包括数据钻取分析等；

4．作为采集监控域的生产库，接收大数据平台计算分析结果，原则上不承担计算任务。

(3) 大数据平台主要承担以下几个作用：

1．接收数据采集缓存和计算结果的缓存减少数据迁移，用于大数据计算；

2．可作为分析型数据库（实时数据仓库）的数据访问补充，即可以直接访问大数据的数据存储提供给应用范围，支撑对访问时间要求不高的业务；

3．优先作为归档数据同步的数据源。

计量自动化系统 3.0 的数据库同步组件应支持主动访问源端数据库，实现实时数据同步。

6.3.2 数据流图

计量自动化主站系统负责实现海量数据的计算和存储。海量数据计算包括实时流式计算和非实时批量计算，计算的结果将分别存储于分布式关系数据库和非关系数据库。为提高分布式关系数据的性能，典型的档案和采集计算数据流图如下，具体随技术选型的逐步明确而进一步的细化和优化调整。

(1) 档案数据流

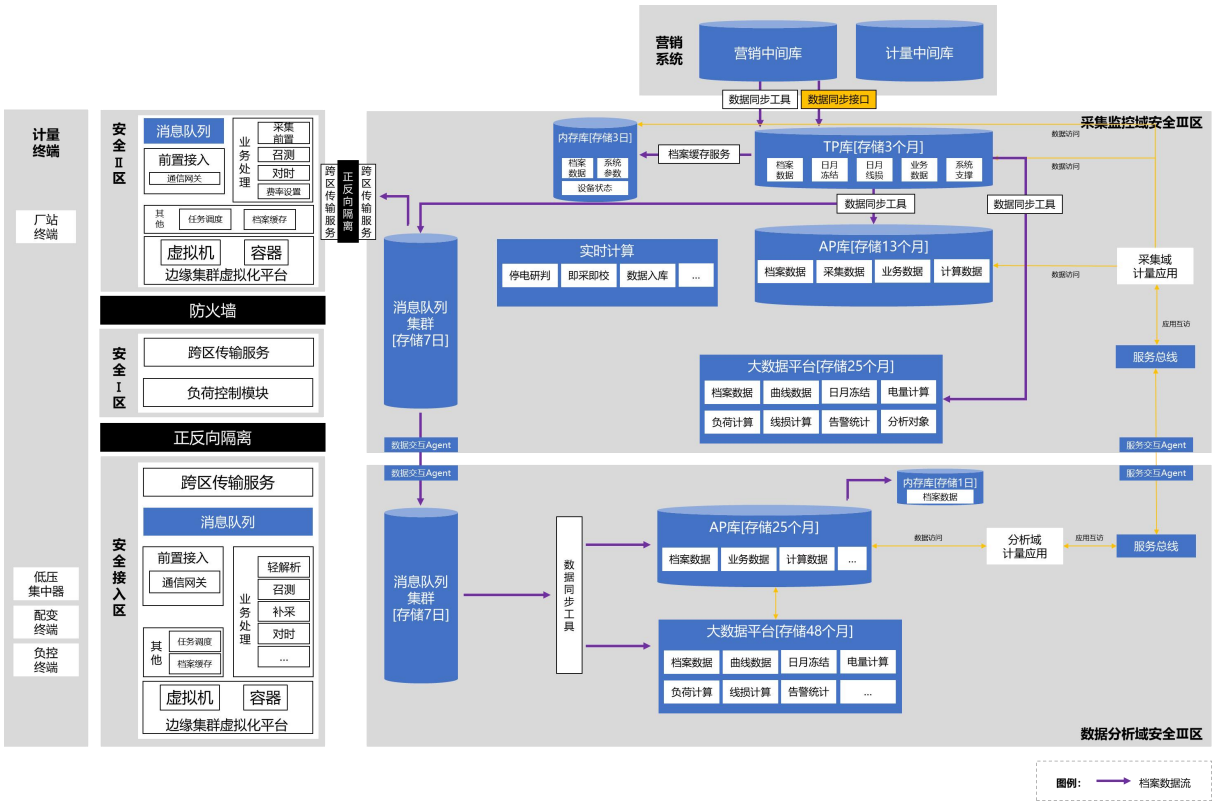

图 6-2 典型档案数据流图

(2) 采集计算数据流

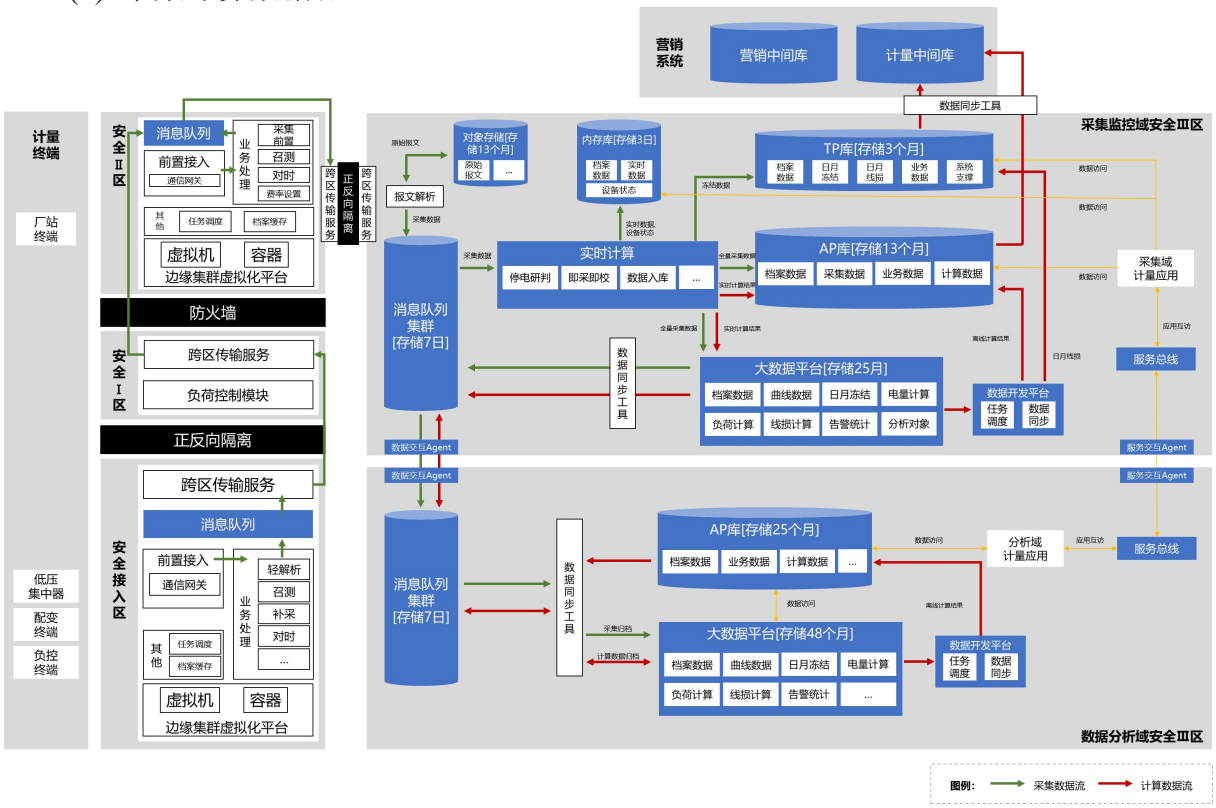

图 6-3 典型采集和计算数据流图

6.3.3 存储架构

6.3.3.1 数据分类

根据计量自动化系统 3.0 业务特点，将数据分为档案类数据、分钟级数据、曲线类数据、冻结类数据、计算类数据、事件类数据、报文类数据、系统管理类数据，数据分类如下图所示：

图 6-4 数据分类设计

6.3.3.2 存储策略

计量自动化系统 3.0 数据库主要包括事务型关系数据库（TP 库）、分析型数据库（AP 库）、内存数据库和非关系数据库等数据存储。初步设计中仅规划了各个数据库的存储空间，数据库的存储空间具体使用须实施阶段主站应用厂家与平台厂家深入沟通后进一步细化，包括读写分类、分库分表等，结合业务的拆分实现最优的业务解决方案，建议对按照业务的聚合对数据库进行物理分库，并根据实际业务需求进一步优化数据流和存储策略。

综合考虑 TP 库、AP 库、非关系型数据库、内存数据库等存储成本、并发能力、分析能力，结合数据特征，建议按照以下原则进行查询优化。

档案模型包括基础档案、分析对象、线损模型、业务事件等数据，该类数据的特征是在页面查询中以多表关联查询（关联采集数据、计算结果数据）为主，页面查询响应时间一般要求在 3 秒内，故档案模型的查询建议存储在 TP 库实现。

实时数据包括分钟级表码、电压电流、功率、设备状态等数据，该类数据的特征是数据量大，当天数据查询的热度高（并发查询较多），且页面查询响应时间一般要求在3秒内，故实时数据的查询建议在内存数据库和AP库实现，其中针对当日实时数据、设备状态的查询及加速前台页面展示通过内存数据库实现，其他实时数据查询通过AP库实现。

曲线数据包括电能示例值曲线、电压电流曲线、功率曲线等数据，该类数据的特征是数据量大，但不涉及高并发查询，且页面查询响应时间一般要求在3秒内，故曲线数据查询建议在AP库实现。

冻结数据包括日月冻结表码和日月最大需量等数据，该类数据特征是按日月存储，数据量一般，涉及多表关联查询，查询的并发量相对其他业务更多，且页面查询响应时间一般要求在3秒内，故冻结数据查询建议在TP库中实现。

计算结果数据包括日月线损数据、计算电量数据、计算负荷数据、指标数据等，其中日月线损数据的数据量不大，但计算较为复杂，适合用大数据平台计算，且页面查询响应时间一般要求在3秒内，故日月线损数据的查询建议在TP库中实现。其他计算结果建议通过AP库实现查询。

事件数据包括设备告警、主站告警等数据，该类数据的特征是数据量较大，涉及关联查询与分析，且页面查询响应时间一般要求在3秒内，故事件数据查询建议在AP库中实现。

事务型业务数据包括召测数据、工单数据、终端版本数据等，该类数据的特征是数据量不大，多为多表关联查询，且页面查询响应时间一般要求在3秒内，但需要数据库支持事务管理，故事务型业务数据的查询建议在TP库中实现。

非事务型业务数据包括计量运行统计分析数据、营业管理统计分析数据、综合能源统计分析数据、智能运维统计分析数据等，该类数据的特征是数据量略大，多为分析计算的结果数据（计算的源数据仍为AP库），对事务功能无要求，且页面查询响应时间一般要求在3秒内，故非事务型业务数据的查询建议在AP库中实现。

系统支撑数据包括系统权限、标准编码、系统参数等数，该类数据的特征是数据量小，并发查询较多，且页面查询响应时间一般要求在1秒内，但需要数据库支持事务处理，故系统支撑数据的查询建议在TP库中实现。

终端报文数据一般指终端上报给计量主站的原始字节流数据，该类数据的特征是数

据量大，查询方式较为单一（由程序实现），不涉及单表查询或多表关联查询，对事务功能无要求，故终端报文数据的查询建议在对象存储中实现。

注：以上存储容量和存储策略会随技术选型的逐步明确而进一步的细化和优化调整。

6.4 计算架构

6.4.1 整体架构

本项目主站涉及实时流式计算和非实时批量计算应对不同的业务场景。

边缘集群计算主要采用采集监控域的数据计算组件，包括实时流式计算和非实时的批量计算，如贵州电网全量计量点电量计算，分析对象电量汇总计算、负荷叠加计算、电能质量数据计算、线损计算等任务，并同时将计算后数据写入分析型数据库中。

实时计算引擎从消息队列中订阅分钟级数据进行实时计算，支撑时延敏感、需要高频计算类业务功能，并将实时计算分析结果实时同步到 AP 库、大数据平台中。

离线计算引擎从大数平台中定时抽取分钟、日、月等数据进行离线计算，支撑时延不敏感、非实时类计算、分析等业务功能，并将离线计算结果定时同步到 TP 库、AP 库、大数据平台中。

边缘集群中实时性比较强的数据流通过实时流式计算，计算结果入到分析型数据库中，实时性要求较低允许一段时间延时的计算通过非实时批量计算，计算结果入库到事务型关系数据库、分析数据库和数据计算组件中的非关系存储中。

本项目原则上两个域数据计算不得使用存储过程进行各类数据的计算，特殊情况下须获得业主认可后才能实施。

6.4.2 实时流式计算

实时流式计算采用流计算框架作为计算处理引擎。相对于批处理，流计算更加强调计算数据流和低时延，通过实时订阅的曲线数据、日/月冻结数据、实时上报事件，主动触发计算作业，瞬时输出计算分析结果，如采集数据的即采即校，数据采集完整率统计，实时电量计算，停电事件的智能研判等，实时流式计算体现计量自动化系统 3.0 的及时响应能力。本期实时计算业务场景为即采即校，其他实时计算业务场景需结合业务需求和资源裕度方可实施。

(1) 计算流程

实时计算在技术架构设计上分为三个步骤，数据获取、数据计算、结果输出：

数据获取：流计算引擎支持多种类型的数据源，包括消息队列、数据库、缓存、文

件等。根据系统总体架构设计，计算服务使用消息队列作为接口，满足流计算引擎的接入标准，通过订阅消息队列，可以实时感知数据的变化状态，配合缓存数据库（类似 redis 等组件）的读取操作，可实现对实时计算分析所需数据的全部接入。

数据计算：实时计算的业务执行逻辑在计算作业环节执行，使用流计算引擎提供的作业调度、状态管理、编程模型、容错机制等功能，开发并提交实时计算程序，处理数据接入环节分钟数据、冻结数据、上报事件，并将计算结果反馈至结果输出环节。

根据业务场景和应用的时间响应需求，将不同的实时计算分析逻辑封装为多个实例进行部署（如实时电量计算、异常分析可以作为两个独立的流计算实例进行开发和部署），在逻辑上保持各个实例之间的隔离性，在避免实例与实例之间相互干扰的同时，方便不同业务的升级、运维与管理。

结果输出：流计算引擎支持多种类型的结果输出，包括输出至消息队列、数据库、缓存，或直接输出为文件等。其中，输出至缓存的主要为满足业务应用的实时访问需求；输出至业务库在为计算结果提供持久化存储能力的同时，可通过数据服务为业务应用提供数据访问渠道。

(2) 业务场景

即采即校：流式计算在采集数据中的处理主要包括数据的即采即校，即在数据入库前，进行数据的有效性校验，如数据的合理性（排除表码倒走异常）校验，例如：抄表结算数据（冻结数据等）。

6.4.3 非实时批量计算

非实时批量计算主要提供海量数据分析场景，部分业务对数据的实时性要求不是太高时，可按一定周期进行相关的数据统计分析，以减少数据计算的压力，提升整体计算效能。

(1) 计算流程

主要包含数据准备、批量计算、结果输出三个部分：

数据准备：作为计算的输入，负责为即将开始的计算提供档案数据和所需的原始数据，同时提供零点冻结档案功能。

批量计算：将计算作业拆分成计算任务的特点，将拆分获得的多个计算任务分发到各个工作节点的工作进程上，实现大规模分布式统计计算。

结果输出：主要是将计算作业输出的结果进行汇总，将汇总后的结果分别写入到计

算缓存和关系数据库中。

(2) 业务场景

非实时批量计算适用于业务逻辑固定，且对统计数据的实时性要求不是很高的业务场景。任务启动的周期可按分钟、小时、日等设置，具体参数设置需要根据业务场景和数据的准备情况进行配置。

电量计算：如日、月电量计算，可根据数据采集的情况和业务需要，设置定时批量计算任务，定期刷新统计数据。

线损计算：可根据业务需要和数据准备情况，设置定时批量计算任务，定期刷新线损数据。

指标统计：可按业务管理需要，设置定时计算任务，刷新各类运行指标。

业务分析：可根据业务需要和数据完整情况，设置定时批量计算任务，定期统计各类业务数据，如行业电量分析，区域电量汇总分析等。

6.4.4 计算分类划分原则

实时流式计算一般是由业务变更触发计算场景，在业务频繁变更的场景时，将触发大量的实时计算，给数据库、服务器带来巨大压力，所以在设置实时流式计算时，需要考虑计算的压力，与批量计算配合使用，原则上以批量计算为主，流式计算为辅。仅需要秒级响应支持的通过实时计算进行计算。

随着计算资源的提高和业务管理对实时性的更高要求，未来越来越多的非实时批量计算可能转变成实时流式计算。

6.5 物理架构要求

计量自动化系统部署于贵州和棠下两个基地的机房，其中数据分析域通过生产控制云节点扩容建设部署在棠下机房，采集监控域通过建设边缘集群部署在贵州机房。根据南方电网计量自动化系统的安防要求，需要在安全接入区、安全Ⅰ区、安全Ⅱ区、安全Ⅲ区都存放相关服务器设备和安全设备等，计量自动化系统主站在安全Ⅲ区提供业务应用服务和数据服务。

从终端到计量自动化系统的通信网络可以分为两类：一类为二区厂站调度数据网。第二类为移动、联通、电信等无线公共网络（不含 Internet 网络）。无线公共网络需要

先接入安全接入区。安全接入区存放采集相关设备，包括前置采集服务器、负载均衡器、卫星时钟、堡垒机等。安全接入区与安全Ⅰ区通过正反向隔离装置连通。

前置采集服务器采集数据经过隔离装置与安全Ⅰ区的通信服务器进行通信，而控制服务器需要接受控制指令的申请，并且需要人工确认。同时，安全Ⅰ区还有安全相关的堡垒机等设备。

安全Ⅱ区，根据要求主要有厂站前置采集服务器，卫星时钟，通信服务器等设备，为适应贵州部分通过调数网接入的厂站侧专变用户远程费率设置的需求，部署了费控密码机及接口服务器等设备，同时根据安防要求，安全Ⅱ区和安全Ⅲ区根据安全要求配置正向隔离装置和反向隔离装置等设备。

安全 III 区，部署分布式平台软硬件资源，提供包括平台管理、弹性计算、存储服务、网络服务、数据库服务、中间件服务、数据处理服务、安全组件等功能，支撑计量自动化系统海量数据的计算和存储以及对外的业务服务等业务功能的基础软硬件需求，并根据安全的相关要求，配置安全软硬件设备。根据《南方电网公司计量自动化系统及新型电力负荷管理系统网络安全防护专项提升工作方案》，需建设安全Ⅲ区缓冲域，最小化部署缓冲域内功能模块。贵州计量自动化系统 3.0 基于安全Ⅲ区云平台租户资源隔离划分安全缓冲域 VPC，部署接口服务，同时结合云防火墙和安全组等资源与生产 VPC 实现逻辑隔离。

本项目中生产环境要求与开发测试等其他环境，通过租户+资源隔离的方式实现，平台厂家必须保障租户从底层资源到上层的数据和云组件的全方位隔离。平台厂家必须保障开发测试等非生产环境的租户无法访问生产环境业务数据；开发测试等非生产环境网络接入通过专用的网络通道接入到云平台中，不影响生产环境的网络通信正常运行；开发测试环境等非生产环境的资源需要做到资源隔离，不允许对生产环境的正常运行造成影响，例如：测试环境的破化性测试不能影响生产环境的正常运行。本项目采集监控域的非生产环境通过边缘集群安全Ⅲ区的资源隔离实现。

6.6 云边协同方案要求

6.6.1 总体方案要求

贵州电网计量自动化系统 3.0 主站分为数据分析域和采集监控域，其中数据分析域部署在调度云棠下延伸节点，采集监控域部署在边缘集群，两个域数据交互参照调度云平台与边缘集群协同交互规范执行，本期实现应用交互和监控交互，云边交互总体架构

如图 6-5 所示：

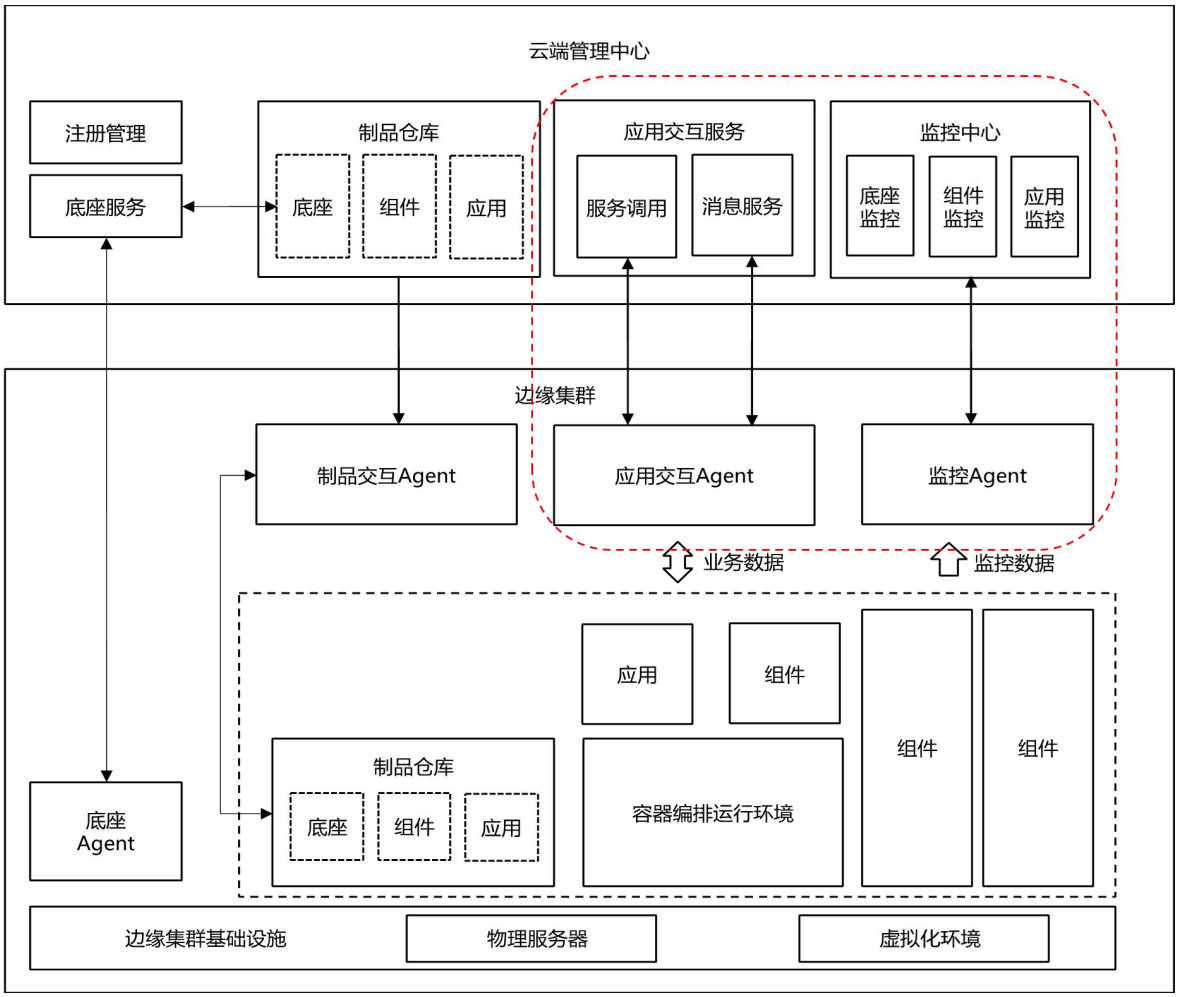

图 6-5 云边交互总体架构

调度云节点的云端管理中心包含注册管理、底座服务、云端制品仓库、应用交互服务和监控中心，本项目涉及的云端管理中心内容如下：

(1) 边缘集群（采集监控域）在云端（数据分析域）注册管理中配置基础信息、网络连接信息。

(2) 依托调度云节点主节点底座服务为边缘集群提供标准底座部署文件，收集边缘集群底座、组件和应用的部署信息。

(3) 云端制品仓库上架标准制品，主站厂家按照调度云节点边缘集群制品开发标准开发完成的底座、组件和应用等制品，可以上架到云端制品仓，本期项目中在实施阶段结合主站业务应用的整体规划细化制品建设内容。

(4) 云端应用交互服务支持调度云节点部署应用与边缘集群部署的应用进行双向交互。本期项目中两个域主要通过应用交互实现主站应用的微服务调用、数据同步等。其中数据同步的方式常用的两种方式，一种通过消息队列进行数据交互为实时性要求比较强的数据提供支撑，一种通过数据库的同步工具实现历史数据的定期同步。

(5) 云端监控中心汇总边缘集群关于底座、组件和应用的监控指标和告警信息，并实现监控指标和告警信息的展示。本项目中各个安全区域的监控信息均会汇聚在边缘集群安全III区的平台监控中，可通过云边协同上报全部的监控信息。

边缘集群具备底座 Agent、制品交互 Agent、应用交互 Agent、监控 Agent 功能，作为与云端管理中心交互的统一出口，实现边缘集群与调度云节点云端管理中心的底座交互、制品交互、应用交互和监控交互。目前边缘集群主要通过安全 III 与云端进行交互，主要涉及交互内容如下：

(1) 底座 Agent 与云端底座服务对接，实现从云端管理中心获取标准底座部署文件、向云端管理中心上报边缘集群底座、组件和应用的部署信息。本项目实现云端的注册信息后，根据实时性要求上报相关信息。

(2) 制品交互 Agent 与云端制品仓库对接，负责云边制品传递。本期项目在实施阶段结合主站业务应用的整体规划细化制品建设内容。

(3) 应用交互 Agent 与云端应用交互服务对接，支撑云边两侧的应用交互需求。本项目主要实现主站应用的数据交互，满足数据分析域与采集监控域的数据交互，满足微服务之间的数据交互及两个域的数据同步。

(4) 监控 Agent 与云端监控中心对接，向云端管理中心上报边缘集群底座、组件和应用的监控指标和告警信息。本项目全部区域的监测信息汇聚至边缘集群的安全III区后，统一上送至云端监控中心。

6.6.2 应用交互

云边协同中应用交互式是两个域重要的交互内容，支持同步和异步两种交互方式，云边应用统一转换成消息的格式来进行交互，消息支持策略配置进行控制，通过配置策略实现消息路由转发。边缘侧部署应用交互 agent，边侧所有的应用交互都通过 agent 进行交互控制，云边应用同步交互架构如图 6-6 所示：

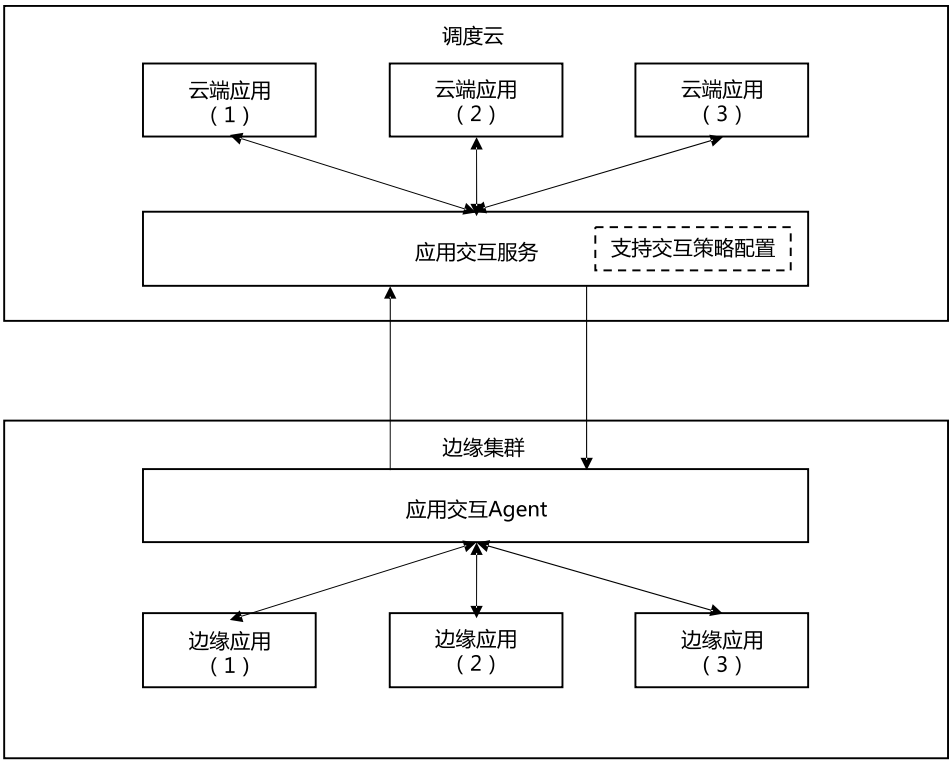

图 6-6 应用同步交互架构图

边缘集群应用交互 Agent 功能包括如下：

(1) 能够支持通过安全管道和云端保持长链接通信能力；

(2) 能够根据云端下发的交互策略启动相应的交互策略服务，为边缘应用提供和云端通信能力的访问地址；

(3) 能够代理边缘集群提供一个统一的外部访问出口。

应用交互支持发布边缘集群在云端运行的应用交互服务，用于与边缘集群的应用交互 Agent 进行对接；在云端运行的应用交互服务可以对边缘集群进行统一的监控、流量管控和交互策略配置。本项目中两个域的数据通信通过云边协同的应用交互实现主站应用程序和数据库等不同之间的应用数据交互，主要采用消息队列方式进行数据交互，对于数据库同步方式，主要通过应用交互实现用户的鉴权和认证后通过数据库同步工具实现。在主站业务应用交互主要场景如下：

(1) 边缘集群历史数据查询，边缘集群中的主站业务应用会调用调度云节点中的数据服务进行前台页面的历史数据展现；

(2) 边缘集群的微服务调用，边缘集中通过微服务接口调用调度云节点的服务，实现业务功能的融会贯通，例如：线损异常分析调用调度云节点中的计量装置异常分析业务应用功能。

(3) 边缘集群的数据同步，边缘集群中的档案数据、采集数据及基础的计算结果同步至生产控制云节点。

(4) 调度云节点跨域计算，调度云节点通过跨域计算调用边缘集群的计算能力实现历史数据计算的任务分解。

(5) 调度云节点为服务调用，通过微服务接口调用边缘集群中的业务功能，实现业务功能的互通，例如：趋势分析中关于当前实时数据展现的页面等。

6.6.3 网络要求

云边协同的通信通道用于调度云节点和边缘集群的数据同步和数据交互，该通信通道本期设计指标为双通道，每条通道带宽 10000Mbps，时延 100ms，相关通信通道由配套机房和通信工程提供，本项目应在通信通道基础上实现云边协同的网络要求。

(1) 能够支持通过安全管道和云端保持长链接通信能力；

(2) 能够根据云端下发的交互策略启动相应的交互策略服务，为边缘应用提供和云端通信能力的访问地址；

(3) 能够代理边缘集群提供一个统一的外部访问出口。

6.6.4 边缘自治

离线状态下边缘集群和业务应用保持正常运行，边缘集群具备自主部署容器组件、镜像仓库、应用能力。要求如下：

(1) 边缘集群本地预置管控服务，可在云边断连离线状态下对边缘节点执行管理操作；

(2) 边缘集群从生产控制云节点上获取本地组织架构信息，并且定期与调度云节点组织架构进行数据同步；

(3) 边缘集群具备本地权限体系，具备独立运行的能力。支持从调度云节点同步组织和权限体系。在与云端断链的情况下，可以独立运作；

(4) 边缘集群规划独立的开发环境和运行环境；

(5) 边缘集群要求具备本地统一的运维管理系统，支持边缘集群的运维管理。

6.7 安全架构要求

安全防护总体目标，贯彻落实电力监控系统“安全分区、网络专用、横向隔离、纵

向认证”十六字方针和安全等级保护三级“一个中心、三重防护”目标以及商用密码应用安全性评估第三级要求等，软硬件设备应当满足国产安全自主可控要求。

电力监控系统的安全防护在安全区域内的安全防护均要满足等级保护和商密的要求，以及“安全分区、网络专用、横向隔离、纵向认证”十六字方针。

按安全分区原则，计量自动化主站各功能模块分别置于不同的安全区。其中置于安全接入区的主要包括采集服务、采集处理服务、密码接口服务、通信服务；置于安全Ⅰ区的主要包括通信服务、控制类业务处理服务；置于安全Ⅱ区的主要包括采集服务、通信服务、采集处理服务（厂站）、非控制类业务处理服务；置于安全Ⅲ区主要包括数据库服务、通信服务、数据处理服务。

计量自动化系统主站系统采集监控域包括安全接入区、安全Ⅰ区、安全Ⅱ区、安全Ⅲ区，各安全大区之间用物理隔离装置隔离，各安全大区内采用防火墙逻辑隔离。主站系统的网络通道主要为电力公司专有的通信网络。以上区域内安全防护应满足等级保护第三级安全要求、商用密码第三级密码应用基本要求、电力监控系统网络安全要求等。

安全防护技术中密码技术需采用国家商用密码算法产品和技术。

安全技术方案要求详见本技术规范书安全技术方案要求章节。

6.8 计量典型场景技术解决方案要求

6.8.1 实时复杂数据分析查询

传统数据库 Oracle 是关系型数据库，不擅长海量数据的在线分析查询。Hbase 等非关系数据库能解决入库效率问题但只能点查和简单关联不支持在线分析和复杂计算场景，且 Hbase 存在写入热点问题，易造成分区服务器不稳定和宕机。Hbase 不能支持实时线损率计算，不能支持电量的在线分类统计，不能支持实时台区用电统计分析等场景，无法直接替代 Oracle 类似的混合数据库应用场景。

当前的解决方案常见是通过异构数据库组合达到取代 Oracle，并在此基础上通过产品的优化和磨合实现超越。

一是通过国产数据库事务型关系数据库实现替代 Oracle 的事务处理能力，兼容 Oracle 语法，保障基于 Oracle 的应用无缝迁移。二是在流批一体计算平台的基础上，建立分析型数据库，采用实时数仓技术（分析型关系数据库中一种），将大量原来由 Oracle 承担的实时分析型 OLAP 业务转移到分析型关系数据库处理，降低对关系事务型数据库的依赖；分析型关系数据库要能实现存储计算分离、实现同时对行存列存的支持、相比

Hbase 的简单点查实时数仓要能实现强事务同时保障丰富的查询能力、性能上要能满足实时查询及分析亚秒级响应；千亿/万亿级数据实时查询及分析秒级响应，能满足全量低压用户分钟级数据采集和实时分析，解决传统架构和开源架构无法解决的问题。

6.8.2 超大规模存储与计算

超大规模存储与计算场景对技术平台的完整性、稳定性、规模性提出了极高要求。一是需要提供关系型存储、列式存储、实时分析型存储、离线分析型存储、对象存储、块存储、文件存储。二是需要有成熟稳定的集群化技术积累，保障能够在一个大规模集群下实现计算任务统一调度的算力规模。三是需要有稳定可靠的 10PB 级存储规模。

平台厂家提供的解决方案需要满足超大规模存储与计算场景的需求，计算存储与大数据存储（历史数据库）应采用成熟稳定并且经过超大规模实践的平台运行，具备稳定性保障和技术持续演进的支持。

6.8.3 完善的数据处理链路

平台厂家提供的解决方案需要按照总体架构中的要求：

(1) 支持实时数据链路、保障数据的即席入库和查询。

(2) 支持离线数据链路、保障归档数据的全局性和一致性。

(3) 支持数据处理链路支持多种数据处理方式。

6.8.4 平台容灾与安全

在安全方面应满足等保三级要求、电力监控系统安全防护要求及商密安全要求。平台提供的所有技术和组件都必须具备自主知识产权，符合国家相关政策标准，能够很好地适应计量自动化系统 3.0 平台级安全要求。

6.8.5 应用管理发布需求

一是要实现计量自动化系统数据分析域与采集监控域的应用架构统一，技术标准统一，系统风格统一，管理模式统一。实现统一可控，两域灵活敏捷的系统运行目标。二是需要分布式编译技术保证下发源代码或镜像，在两域各自编译或发布。

构建自动化发布流程，实现两域的自动化打包发布，提供多种发布策略，包括滚动发布、多活、灰度等。开展项目研发全过程管理、在线自动化测试、一键发布部署等活动，既解决研发测试部署过程中的“两张皮”问题，也解决统一版本发布的应用发布问题。

6.8.6 安全自主可控需求

计量自动化系统 3.0 基础软硬环境应适配国产芯片、操作系统、数据库以及其他技

术组件等方面提升国产化水平，实现“安全、自主、可控”，为业务部门提供兼容开放、功能一致、稳定可靠、性能优异、安全合规的安全自主可控技术。

6.9 数据一致性要求

计量自动化系统 3.0 主站分为两个域的平台，主站系统的数据存储根据数据特点和计算流程不同，采用了不同的数据库混合数据存储架构，划分了两个域多个区分别存储各项数据，其中档案数据、原始采集数据、计算结果数据都在两个域各个区中同时存储，需要主站应用通过平台提供的数据同步工具、消息队列等技术需要保证各个区域内数据一致性，原则上要求平台提供的数据同步工具数据不丢失，支持数据重传、断点续传等功能。

(1) 档案数据一致性保证

档案数据是计量自动化系统基础数据，需要参与计算，在日常查询统计中需要进行查询关联，对外发布数据往往需要关联档案数据等，为保证数据一致性，需要明确档案数据的统一来源。本项目中档案原则上均来源于营销系统，从营销系统获取档案数据后同步至采集监控域的事务型关系数据库，因此主站系统中档案数据统一来源是营销系统，需要使用档案数据的，原则上需保证主站系统各数据库之间的数据一致性。

(2) 采集数据一致性保证

原始采集数据作为主站系统的核心基础数据，是统计分析和数据计算的基础，为提升计算性能，同时为了保证数据持久化，消息队列作为实时最强的唯一数据源（非发布数据），发布数据以发布库作为唯一的数据来源。原始采集数据通过数据同步工具同步至采集监控域及数据分析域的数据库中，保障数据的一致性。

(3) 计算结果数据一致性保证

计算结果数据指的是电量叠加、负荷极值等从原始采集数据经过初步计算的数据，这些明细数据需要支撑日常统计查询和后续分析汇总应用，它们分布在关系数据库、非关系列式数据库等。为保证数据一致性，计算结果以采集监控域中的数据以分析型分布式关系数据库为准，数据分析域中以历史数据库为准。数据的一致性由主站应用通过数据同步工具负责，主站应用通过数据计算组件计算程序计算或重新计算后更新关系数据库、非关系列式数据库等数据库，原则上不允许运维人员直接修改数据库数据，从而保证数据的一致性。

(4) 一致性、及时性要求

完整性要求：各类异构数据库的档案数据、表码数据等同步保障 100%一致；

及时性要求：各类异构数据库同步 100 万条任何类型的数据，须在 10 分钟内完成。

(5) 数据同步规划要求

根据业务实际情况规划数据同步计划，区分各类数据的重要程度及同步优先级要求，例如档案数据、监控数据等增量变更数据需满足秒级同步，对于统计分析等数据可以延迟一段时间。

6.10 资源共享要求

为了提升资源优化配置能力，要求采用计算虚拟化、存储虚拟化、网络虚拟化等方面的系统关键技术，很好地解决传统系统建设的问题，通过提高物理服务器、存储、网络利用率大幅度削减其购置需求、数量和运营成本；通过利用服务器虚拟化中 CPU、内存、网络、存储等资源的动态调整能力实现对业务应用资源需求的动态响应，提升业务应用的服务质量，提高管理员运维效率，大大降低运维人员的运维工作量。通过在线虚拟机漂移实现更高的可用性和可靠性以及各种基于资源优化或节能减排策略的跨物理服务器的调度等，同时降低硬件采购、部署运维、能耗等方面的成本。

本期项目中由平台提供虚拟机、容器等资源供主站业务系统需要的共享资源，如接口服务、文件传输服务等需要虚拟机或容器，原则上要求主站厂家在调度云节点和边缘集群均采用容器化技术部署应用程序。

6.11 可靠性保障方案要求

6.11.1 计量自动化系统分布式平台可靠性

分布式技术解决了可扩展性问题，但带来了集群管理、资源调度、数据同步等需求。这些能力可以通过单集群最大可扩展规模等指标衡量。计量自动化系统分布式平台应有大规模落地案例，并通过国家或行业权威机构检验及评测报告。常见的评测包括工信部电信研究院（中国信通院）可信云评估、大数据产品能力测评；工信部、国家标准化委的 ITSS 云计算服务能力；中国电子技术标准化研究院的云基准测评等。本项目中提供的调度云节点及边缘集群中的软件原则上采用大规模落地的云平台原生的产品包括基础设施服务、数据库服务、中间服务等，并与平台厂家的公有云平台产品组件保持一致。

6.11.2 数据库自治能力

计量自动化系统 3.0 采用事务型、分析型、NoSQL 型等多类型的数据库，这些组件多为分布式架构，以满足海量数据存储计算的需要。在满足了扩展性的同时，不可避免带来分布式管理的问题，让数据库的运维和管理常常受到多种挑战。数据库自治服务是一种基于机器学习和专家经验实现数据库自感知、自修复、自优化、自运维及自安全的云服务，帮助用户消除数据库管理的复杂性及人工操作引发的服务故障，有效保障数据库服务的稳定、安全及高效。具体要求见平台建设方案/数据库服务/数据库自治章节。

6.11.3 数据链路可靠性

计量自动化系统 3.0 将原本一个 Oracle 数据库处理的业务分散在多个处理环节，涉及消息队列、实时计算、关系型数据库、分析型数据库、离线计算等多个数据计算组件，极大地提升了计量系统的数据处理能力，但同时也对组件之间的协同提出很高的要求。根据业务要求需要设计数据同步链路的场合，需要平台提供辅助性工具保证数据最终一致性，而不是由上层的应用来实现。具体来说：

离线同步，需支持涵盖关系型数据库、MPP、NoSQL、文件存储、消息流等各大种类数据源的任意的读写组合。

实时同步，需支持业务数据库实时更新入仓，支持消息毫秒级传输。全量/增量一体化实时同步，支持整库/整实例级一次性配置多库多表同步。支持自动进行全量（批量）与增量数据的合并。

离线和实时同步配合实现分库分表同步，自动管理同步任务，自动融合数据，自动兼容新增库表，将分库分表抽象为单一虚拟表，方便管理。

6.11.4 容灾能力

计量自动化系统作为电网核心业务系统，需要考虑容灾建设。本次建设的贵州计量检定中心基地边缘集群需要能支持将来异地容灾的需求，本期采集监控域支持主备采集（降级灾备）。

6.12 边缘集群（采集监控域）运行指标

采集监控域平台指标，需要单机设备指标及软件组件整体指标不低于如下三方面的要求：

(1) 参与南网云边协同技术验证的厂家提供的产品和技术指标不能低于测评结果，未参加南网云边协同技术验证的厂家的技术指标要求不能低于所有参与测试厂家的平

均水平；平台厂家与主站厂家应相互配合系统的投运指标应满足南网计量自动化 3.0 验收质量评价中的相关指标要求；

(2) 满足本章节边缘集群（采集监控域）运行指标提出的指标要求。

6.12.1 整体指标

(1)平台提供服务的平均无故障时间（MTBF）大于 3 万小时；

(2)平台服务的可用性>99.95%；

(3)平台故障恢复时间小于 2 小时；

(4)平台由于偶发性故障而发生自动热启动的平均次数小于 1 次/3600 小时；

(5)单点故障节点为 0；

(6)平台软件版本必须为供应商最新的稳定版本；

(7)安全 II 区、安全接入区等与安全 III 区同类型指标按照单节点的处理性能做线性扩展下的运行指标要求；

(8)全量电能表电量计算平均耗时≤20 分钟；

(9)行业电量计算耗时≤30 分钟；

(10)云边数据一致率≥99.9%；

(11)云边数据同步及时率≥99.9%；

(12)查询运行电能表 30 日内表码的平均耗时≤1 秒；查询低压用户 1 日电压数据的平均耗时≤1 秒。

6.12.2 具体指标要求

6.12.2.1 云平台底座

指标项	具体要求
分布式云操作系统	应支持大集群规模，云平台集群规模最大应支持不少于 5000 台物理服务器。
	应具备高可扩展性，可支持上亿个文件和 PB 以上量级的文件存储；支持不重启系统，增加物理服务器后自动扩容。
租户权限及隔离	平台内的虚拟机、容器、数据库、大数据等各类组件必须支持统一的租户权限认证和资源隔离。其中资源隔离必须满足从物理设备、数据存储、业务应用等几个层次的隔离，不同的租户之间不允许在未得到授权的情况下访问其他租户的硬件资源、数据，不得影响其他租户的正常运行。例如：测试租户的破坏性测试，不得影响生产环境的正常运行。

6.12.2.2 基础设施服务

指标项	具体要求
云服务器	单个云主机能够挂载不低于 16 块数据盘，单个数据盘的存储容量不小于 32TB，实例可挂载的数据盘最大容量不小于 5TB，可以为每块磁盘创建 64 个快照。
	单台虚拟机主动热迁移，网络中断时间＜200ms。
容器服务	Master 节点高可用支持 5 节点和 3 节点模式，5 节点模式下故障 2 台，3 节点模式下故障 1 台，不影响集群正常使用，全部 Master 节点全部故障时，不影响已有业务正常使用。
块存储	在线变规格：支持在不中断业务的前提下，在线变更云盘规格，满足灵活多变的业务需求。
	磁盘容量：单个云盘最高支持 32TB 容量。
对象存储	单个对象支持不少于 48.8TB，单租户支持不少于 100 个 bucket。
NAT 网关	提供不低于 10Gbps 级别的 NAT 转发能力。
云桌面	考虑到桌面之间的切换需求，PC（或笔记本）使用客户端接入，需支持同时打开不少于 30 个云桌面。
	支持至少 4K、60FPS 显示，支持双屏显示。
	支持批量远程开机、重启、关机、释放云桌面，发送远程命令至云桌面。

6.12.2.3 数据库服务

术语定义：

内表：数据库存储的表；

外表：数据库外其它存储的表，元数据集在数据库，数据在数据库外部。

指标项	具体要求
TP 库基本性能	CPU 每核提供不低于 3000 QPS 的简单查询能力，支持水平能力扩展。
	提供同城容灾、异地容灾部署能力，满足不同业务场景的可用性要求。
	管控、内核分离部署，提供业务、运维链路分离的服务等级协议保障机制。
	集群采用多节点冗余架构，无单点故障，支持节点故障服务的自动负载均衡。
	多表数据入库花费总时间：以系统用电客户、计量点、测量点、电表资产、终端 5 种实际数据结构为依据（含主键与索引）创建 5 张数据表，并模拟数据文件（TXT 文件，E 语言格式），从外部写入数据库，能够实现数据入库性能≥15 万条/秒。
	多表入库数据丢失率：以系统用户、计量点、测量点、电表资产、终端 5 种实际数据结构为依据（含主键与索引）创建 5 张数据表，并分别模拟 5 份含 2400 万条记录的数据文件（TXT 文件，E 语言格式，共计 12000 万条记录），从外部入库服务器写入数据库，入库后统计所有入库文件所包含数据记录数，以及数据库内 5 张表全量数据记录数，统计数据丢失率应小于等于 0。
TP 库并发处理能力	单表并发插入数据总消耗时间：以系统测量点实际数据结构为依据（含主键与索引）创建 1 张数据表，并在表内模拟 10 亿条记录数据，使用并发测试工具模拟 50 个用户同时向该表插入 1 条数据，总执行完成时

指标项	具体要求
	间小于 1 秒。
	单表并发修改数据总消耗时间：以系统测量点实际数据结构为依据（含主键与索引）创建 1 张数据表，并在表内模拟 10 亿条记录数据，使用并发测试工具模拟 50 个用户同时修改该表指定不同测量点同一个字段数据（50 个并发用户分别修改 50 个测量点），总执行完成时间小于 2 秒。
	单表并发删除数据总消耗时间：以系统测量点实际数据结构为依据（含主键与索引）创建 1 张数据表，并在表内模拟 10 亿条记录数据，使用并发测试工具模拟 50 个用户同时删除该表不同测量点的 1 条数据（50 个并发用户分别删除 50 个测量点），总执行完成时间小于 1 秒。
TP 库查询能力	并发 100 个用户情况下小数据量单表查询时间（建索引）：以系统采集中高压实时表码数据结构为依据，模拟 10 亿条记录数据，在建索引情况下，模拟 100 个用户同时从该表中查询出指定单个测量点指定单日时间范围内 96 条记录的查询时间小于 3 秒。
	并发 100 个用户情况下大规模数据单表查询时间（建索引）：以系统采集中高压实时表码数据结构为依据，模拟 1 亿条记录数据，在建索引情况下，模拟 100 个用户同时从该表中查询出指定时间范围内结果集 2348 万条记录，并输出前 100 条（row1 至 row100）的查询时间小于 5 秒。
	并发 100 个用户情况下数据分组排名查询时间（建索引）：以系统低压居民用户、计量点、测量点、电表资产、日表码 5 个表数据结构为依据，各模拟 2400 万条记录数据，在所有表建索引情况下，模拟 100 个用户同时对 5 个表进行关联查询并按用户进行分组求和并排序，输出前 100 条记录（row1 至 row100）的花费时间小于 5 秒。
	并发 100 个用户情况下大规模数据联合查询时间（建索引）：以系统中高压用户、计量点、测量点、电表资产、实时告警 5 个表数据结构为依据模拟记录数据，其中包括用户、计量点、测量点、电表资产、实时告警，在所有表建索引情况下，模拟 100 个用户同时对 5 个表进行关联查询，查询出指定单日内结果集 100 万条告警数据，输出前 100 条记录（row1 至 row100）花费时间小于 5 秒。
分析型数据库（AP 库）基本性能	生产环境单集群可支持单库不少于 1PB 数据量。 生产环境支持亿级数据表查询与关联分析。
分析型数据库（AP 库）入库能力	在 Merge 强约束条件下，将 26 列 800 万记录入库到 3100 亿记录的 AP 库内，入库速度不低于 260 万行每秒。
分析型数据库（AP 库）存储能力	存储副本：支持分布式多副本存储模式，且不少于指标阈值要求副本数量；支持副本数据自动同步管理，确保多副本数据一致性；支持副本负载均衡，多个用户访问同一个数据可负载均衡到多个副本中取数。
分析型数据库（AP 库）读写并行能力	基于 Merge 模式实现 1 天的负荷数据入库（109 亿行），写入【读写表】（3100 亿）；同时基于【读写表】开展复杂查询测试，数据入库和复杂查询操作需要并行执行。
	在 Merge 强约束条件下，将 109 亿记录入库到 3100 亿记录的 AP 库内，入库速度不低于 260 万行/秒。

指标项	具体要求
	在强约束条件下，100 并发，多表关联查询，查询一条记录，数据表【档案宽表】和【读写表】关联查询（千亿级记录数），复杂查询耗时 30 秒内。
分析型数据库（AP 库）查询能力	在强约束条件下，100 并发，多表关联查询，按照【电能表标识+数据时间】查询一条记录，数据表【组织机构 + 用电用户 + 计量点 + 运行电能表（测量点）+ 电能表资产】（千万级记录数）和【1 天电能表负荷数据基准表】（百亿级记录数）关联查询，总耗时 5 秒内。
内存数据库	主从版可支持不少于 64GB 缓存容量，集群版可支持不少于 1TB 缓存容量，集群版可支持不少于 128 个分片节点，当一套不支持本项目所需的内存库存储规模时，需提供多套，以满足项目需求。
数据库备份	支持不低于每秒 10GB 数据备份速度。
	数据库备份必须支持物理备份和逻辑备份，且不能采用灾备的形态替代数据库备份。
数据库自治	支持 10 秒 SQL 分析功能，在 10 秒中，每隔一秒钟，执行一次查看 SQL 任务进程，然后将所有的结果集进行统计分析。
	支持实时性能，提供通过图标或者黑屏的方式，每隔 5 秒自动采集数据库性能信息，有效地帮助数据库盯屏和护航。
	数据库自治必须能够自动实现表空间自动收缩、垃圾自动清理、统计信息自动解析等，且需要支持在线的资源回收和处理。

6.12.2.4 中间件服务

指标项	具体要求
企业级分布式应用服务（微服务）	提供批量运维功能，可以对集群、应用以及指定的机器节点批量执行运维命令。
	支持国产化集成开发环境，支持插件一键部署应用。
应用实时监控	提供线程粒度的 CPU 耗时和每类线程数量的统计，可以根据 CPU 耗时统计快速发现异常线程。
云服务总线	无间断扩容：支持服务总线节点的无间断扩容，能够水平扩展服务总线节点，线性增加服务能力。
日志服务	日志服务支持通过密钥管理服务对数据进行加密存储，提供数据静态保护能力。支持使用托管密钥进行加密。支持通过用户自带密钥（BYOK）加密。
	支持千亿日志查询的秒级返回。

6.12.2.5 数据计算处理

指标项	具体要求
实时计算	生产环境单集群支持不少于 2000 个运行作业。
	生产环境计算集群可扩容至不少于 500 台物理服务器。
	生产环境单作业吞吐量可达每秒 800 万条。
	生产环境单集群吞吐峰值可达亿级别规模。
离线计算	支持超大规模的 MapReduce 计算，可支持最大 Mapper 个数为 10 万，

指标项	具体要求
	最大 Reduce 个数为 1000，最大 Join 个数 1 万。
	超大规模节点调度能力，具备万级节点以上调度能力。
	大数据计算平台能力单集群可达到 5000 台物理服务器并行作业。
	离线计算支持秒级查询，不依赖外部引擎。
	计算平台处理一天历史数据全部计算任务时间小于 30 分钟。
	计算平台处理一个月历史数据全部计算任务时间小于 12 小时。
分布式消息队列	数据处理能力不小于 40KQPS
数据开发组件	支持国内主流数据库类型，丰富数据开发、处理能力。
数据管理组件	支持动态扩缩容数据计算组件的集群。
数据同步能力	采集监控域与数据分析域之间的一天内的全量数据同步时间不超过 30 分钟，确保数据无积压，若有积压，需通过应急处理方案对数据进行紧急处理。
	数据计算组件分布式非关系数据库与采集监控域分析型关系数据库之间的一天内的全量数据同步时间不超过30分钟，确保数据无积压，若有积压，需通过应急处理方案对数据进行紧急处理。
	数据同步丢失率为 0。
	不同数据库之间要支持大批量和增量数据的自动同步，保持数据一致率 100%。

7 详细技术方案要求

7.1 硬件设备技术要求

7.1.1 使用条件

7.1.1.1 正常工作大气条件

(1) 环境温度：-10℃～+55℃；

(1) 相对湿度：5%~95%(产品内部既不应凝露，也不应结冰)；

(2) 大气压力：80kPa～106kPa。

7.1.1.2 贮存、运输环境条件

(1) 设备在运输中允许的环境温度-40℃～＋70℃，相对湿度不大于 85%；

(2) 在贮存中允许的环境温度-25℃～＋55℃，相对湿度不大于 85%，在不施加任何激励量的条件下，设备不出现不可逆变化。

7.1.1.3 周围环境

(1) 场地符合 GB/T 9361-2011 中 B 类安全要求；

(2) 使用地点不出现超过 GB/T 11287 规定的严酷等级为 I 级的振动；不发生 GB/T 17742－2008 规定的烈度为Ⅶ度的地震；

(3) 使用地点无爆炸危险的物质，周围介质中不含有能腐蚀金属、破坏绝缘和表面敷层的介质及导电介质，没有严重的霉菌存在。

7.1.1.4 电源条件

(1) 电压：200V~240V，正弦交流电。

(2) 频率：50±0.2 Hz。

(3) 支持两路及以上 UPS 独立供电。

7.1.2 服务器总体参数要求

服务器技术要求中的配置参数为参考配置，投标方提供的服务器总的配置如服务器数量、CPU、内存、存储、网络等均应大于等于下面清单中的参数，否则视为负偏差。

本项目各安全区服务器整体要求如下表所示，各款机型详细配置详见下文。

服务器整体要求	具体的服务器数量及配置，需满足本项目系统的资源需求及技术指标要求，并参照技术验证结果配置。 服务器均需满足以下要求： 1、操作系统兼容性：支持统信 UOS，银河麒麟等安全自主可控操作系统。 2、远程管理：支持虚拟 KVM 功能，可实现与操作系统无关的远程对服务器的完全控制。 3、虚拟化支持：支持 KVM 等主流虚拟化技术。 4、CPU 和操作系统等关键部件应当符合安全可靠测评要求。 5、厂商需提供中国质量认证中心（CQC）颁发的 CCC 现场检测实验室证书； 6、服务：提供芯片原厂供货保障承诺函，五年原厂质保服务，需提供生产厂家开具的质保函及售后服务承诺函；原制造商提供 5 年免费上门维修服务，人工、配件、交通等任何费用全免(硬盘保留)。 7、响应级别要求：7X24 小时，30 分钟内响应，4 小时内工程师携备件到达现场，8 小时内解决硬件故障。 8、应满足附件 3《政府采购需求标准》中对应投标产品形态的技术参数要求。

7.1.3 安全III区

7.1.3.1 资源要求

(1) 采集监控域存储资源要求

根据资源配置基本原则，现有各类型用户总数及未来 5 年的用户增量情况，结合各类型用户的采集频率，按照业务存储需求分别进行原始报文存储、入库缓存存储、采集数据库存储、数据计算组件存储、应用数据库存储、文本对象存储、虚拟机存储等各类型存储需求，进行详细的存储资源需求估算。

本期项目边缘集群安全III区存储资源要求如下：

存储需求分类	需求说明	存储类型	总可用容量（TB）	最大存储周期		高性能（内存）	高性能（SSD）	一般性能（HDD）
				时长	单位			
数据总线存储需求	原始报文文件+采集数据	消息队列	19.25	7	日		19.25	
内存数据库存储需求	计算、业务数据+档案数据	内存库	3.64	3	日	3.64		
AP 库存储需求	采集、计算、业务数据	关系分析型数据库（AP 库）	1151.5	13	月		1151.5	

存储需求分类	需求说明	存储类型	总可用容量（TB）	最大存储周期		高性能（内存）	高性能（SSD）	一般性能（HDD）
				时长	单位			
TP 库存储需求	计算、业务数据+档案数据	关系事务型数据库（TP 库）	82.25	3	月		82.25	
大数据计算存储需求	采集、计算、业务数据	非关系数据库	2096.60	25	月		157.25	1939.36
对象存储需求	原始报文文件+图文文件+AP 库备份	对象存储	587.52	13	月			587.52
块存储	虚机、容器、云桌面、日志等	分布式存储	141	长期			141	
合计			4081.76					

注：存储资源的具体形态和用途需在实施阶段根据平台产品特性和主站应用的需求选择具体的存储类型。存储资源的可用容量不得少于需求容量，内存规格原则上不得低于 DDR4，频率不低于 2933MHz；除系统盘外，高性能（SSD）介质类型原则上应为 NVME PCIE SSD 硬盘或 SATA SSD，并可根据业务需求配置读取密集型或读写混合型；一般性能（HDD）介质原则上应为 SAS HDD/SATA HDD，硬盘转速不低于 7200RPM。实际配置时，大数据计算及块存储应将热数据优先存储于高性能介质内，将温数据存储于一般性能介质内，以满足系统生产的性能需要。

7.1.3.2 可用容量计算

组件名称	要求授权量	授权单位	数量	设备类型	可用容量计算
云服务	6136	逻辑核	52	底座型服务器	单台服务器可提供的有效 vCPU 是 118 vCPU，总的有效 vCPU= 单机提供 vCPU[118Core]*服务器数量[52]=6136vCPU
对象存储	587.52	TB	16	存储型服务器-2	3 副本：单台可用存储容量=单台服务器磁盘物理容量[144T]*磁盘格式化损耗[0.9] *水位线[0.83] /副本数[3] =36.72T 总的可用容量=单台可用存储容量[36.72T] *服务器数量[16] = 587.52TB EC：单台可用存储容量=单台服务器磁盘物理容量[144T]*磁盘格式化损耗[0.9] *水位线[0.83] * EC 容量利用率[0.6666] =71.70T 总的可用容量=单台可用存储容量[71.70T] *

组件名称	要求授权量	授权单位	数量	设备类型	可用容量计算
					服务器数量[16] = 1147.2TB
块存储	141	TB	12	存储型服务器-1	3 副本：单台设备可用存储容量=单台设备磁盘物理容量[46.08T] * 数据磁盘占比[1.0] * 水位线[0.85] *磁盘格式化损耗[0.9] /副本数[3] = 11.75TB 总的可用容量=单台可用存储容量[11.75T] * 服务器数量[12] = 141TB EC：单台可用存储容量=单台服务器磁盘物理容量[46.08T]*磁盘格式化损耗[0.9] *水位线[0.83] * EC 容量利用率[0.6666] =22.95T 总的可用容量=单台可用存储容量[22.95T] * 服务器数量[12] = 275.4TB
分析型数据库	1151.5	TB	98	数据库型服务器	3 副本：单台设备可用存储容量=单台设备磁盘物理容量[46.08T] * 数据磁盘占比[1.0] * 水位线[0.85] *磁盘格式化损耗[0.9] /副本数[3] = 11.75TB 总的可用容量=单台可用存储容量[11.75T] * 服务器数量[98] = 1151.5TB 2 副本：单台可用存储容量=单台服务器磁盘物理容量[46.08TB] * 数据磁盘占比[1.00] * 磁盘格式化损耗[0.9] *水位线[0.85]/副本数[2] =17.62TB 总可用存储容量=单台可用存储容量[17.62TB] * 服务器数量[98] = 1726.76 TB
事务型关系型数据库	82.25	TB	7	数据库型服务器	事务型关系数据库应以集群形式部署。 不含 RAID 方式：单台服务器磁盘物理容量[46.08T] * 数据磁盘占比[1.0] *水位线[0.85] *磁盘格式化损耗[0.9] /副本数[3] = 11.75TB 总的可用容量=单台可用存储容量[11.75T] * 服务器数量[7] = 82.25TB 含 RAID 方式：单台服务器磁盘物理容量[46.08T] * RAID 利用率[0.75] * 数据磁盘占比[1.0] *水位线[0.85] *磁盘格式化损耗[0.9] /副本数[3] = 8.81TB

组件名称	要求授权量	授权单位	数量	设备类型	可用容量计算
					总的可用容量=单台可用存储容量[8.81T] * 服务器数量[7] = 61.67TB
内存数据库	3727.5	GB	10	性能型服务器-2	单台可用内存容量=(单台服务器内存物理容量[1024G] - 系统保留容量[30G]) * 内存水位[0.75] / 副本数[2] =372.75G 总可用内存容量=单台可用内存容量[372.75G] * 服务器数量[10] = 3727.5G
分布式消息队列	58.8	TB	10	大数据型服务器	单台服务器吞吐量 = 服务器处理量[110MB/s] * 系统预留[0.85] = 93.5MB/s 总的服务器吞吐量=单台服务器吞吐量[93.5MB/s] * 服务器数量[10] = 935MB/s 单台可用存储容量=单台服务器磁盘物理容量[23.04] * 磁盘格式化损耗[0.90] * 水位线[0.85] / 副本数[3.0] = 5.88T 总可用存储容量=单台可用存储容量[5.88T] * 服务器数量[10] = 58.8T
实时计算	2400	逻辑核	25	大数据型服务器	单台逻辑核 = 96 逻辑核 总的逻辑核 = 单台逻辑核[96] * 服务器数量[25] = 2400 逻辑核
离线计算	2112	逻辑核	22	大数据型服务器	单台逻辑核 = 96 逻辑核 总的逻辑核 = 单台逻辑核[96] * 服务器数量[22] = 2112 逻辑核

注：配置清单仅作参考，实际计算、存储资源配置以技术验证选型后配置为准。

7.1.3.3 服务器技术要求

每台服务器配置≥2 路热插拔电源，每单路热插拔电源可满足设备满载运行要求，任意一路电源故障设备功能应不受影响。

7.1.3.3.1 底座型服务器

服务器类型	配置
底座型	1、2U 机架式服务器； 2、CPU: 配置≥2 颗安全自主可控 CPU；单颗 CPU 要求：X86 架构核数≥24，主频≥2.2GHZ 或 ARM 架构核数≥48 核，主频≥2.6GHZ； 3、内存：内存容量≥512GB，类型 DDR4 及以上，频率≥2933MHZ； 4、系统盘：配置≥960GB SSD【2*480GB SSD】硬盘； 5、数据盘：≥7.68TB SSD+96TB HDD； 6、网络：配置≥2*双光纤端口 25GE 以太网卡（含光模块）； 7、电源：配置≥2 路热插拔电源，每单路热插拔电源可满足设备满载运行要求，任意一路电源故障设备功能应不受影响。

7.1.3.3.2 通用型服务器

服务器类型	配置
通用型	1、2U 机架式服务器； 2、CPU: 配置≥2 颗安全自主可控 CPU；单颗 CPU 要求：X86 架构核数≥32，主频≥2.6GHZ 或 ARM 架构核数≥64 核，主频≥2.6GHZ； 3、内存：内存容量≥512GB，类型 DDR4 及以上，频率≥2933MHZ； 4、系统盘：配置≥960GB SSD【2*480GB SSD】硬盘； 5、网络：配置≥2*双光纤端口 25GE 以太网卡（含光模块）； 6、电源：配置≥2 路热插拔电源，每单路热插拔电源可满足设备满载运行要求，任意一路电源故障设备功能应不受影响。

7.1.3.3.3 性能型服务器

服务器类型	配置
性能Ⅰ型	1、2U 机架式服务器； 2、CPU: 配置≥2 颗安全自主可控 CPU；单颗 CPU 要求：X86 架构核数≥32，主频≥2.6GHZ 或 ARM 架构核数≥64 核，主频≥2.6GHZ； 3、内存：内存容量≥1024GB，类型 DDR4 及以上，频率≥2933MHZ； 4、系统盘：960GB SSD【配置≥2*480GB SSD】硬盘； 5、网络：配置≥2*双光纤端口 25GE 以太网卡（含光模块）； 6、电源：配置≥2 路热插拔电源，每单路热插拔电源可满足设备满载运行要求，任意一路电源故障设备功能应不受影响。
性能Ⅱ型	1、2U 机架式服务器； 2、CPU: 配置≥2 颗安全自主可控 CPU；单颗 CPU 要求：X86 架构核数≥32，主频≥2.6GHZ 或 ARM 架构核数≥64 核，主频≥2.6GHZ；

服务器类型	配置
	3、内存：内存容量≥1024GB，类型 DDR4 及以上，频率≥2933MHZ； 4、系统盘：960GB SSD【配置≥2*480GB SSD】硬盘； 5、数据盘：≥15.36TB NVME SSD【4*3.84TB NVME SSD】； 6、网络：配置≥2*双光纤端口 25GE 以太网卡（含光模块）； 7、电源：配置≥2 路热插拔电源，每单路热插拔电源可满足设备满载运行要求，任意一路电源故障设备功能应不受影响。

7.1.3.3.4 数据库型服务器

服务器类型	配置
数据库型	1、2U 机架式服务器； 2、CPU: 配置≥2 颗安全自主可控 CPU；单颗 CPU 要求：X86 架构核数≥32，主频≥2.6GHZ 或 ARM 架构核数≥64 核，主频≥2.6GHZ； 3、内存：内存容量≥1024GB，类型 DDR4 及以上，频率≥2933MHZ； 4、系统盘：配置≥960GB SSD【2*480GB SSD】硬盘； 5、数据盘：配置≥46.08TB NVME SSD【12*3.84TB NVME SSD】； 6、网络：配置≥2*双光纤端口 25GE 以太网卡（含光模块）； 7、电源：配置≥2 路热插拔电源，每单路热插拔电源可满足设备满载运行要求，任意一路电源故障设备功能应不受影响。

7.1.3.3.5 大数据型服务器

服务器类型	配置
大数据型	1、2U 机架式服务器； 2、CPU: 配置≥2 颗安全自主可控 CPU；单颗 CPU 要求：X86 架构核数≥24，主频≥2.2GHZ 或 ARM 架构核数≥32 核，主频≥2.6GHZ； 3、内存：内存容量≥512GB，类型 DDR4 及以上，频率≥2933MHZ； 4、系统盘：配置≥960GB SSD【2*480GB SSD】硬盘； 5、数据盘：配置≥7.68TB SSD+144TB HDD； 6、网络：配置≥2*双光纤端口 25GE 以太网卡（含光模块）； 7、电源：配置≥2 路热插拔电源，每单路热插拔电源可满足设备满载运行要求，任意一路电源故障设备功能应不受影响。

7.1.3.3.6 存储型服务器

服务器类型	配置
存储Ⅰ型	1、2U 机架式； 2、CPU: 配置≥2 颗安全自主可控 CPU；单颗 CPU 要求：X86 架构核数≥24，主频≥2.2GHZ 或 ARM 架构核数≥32 核，主频≥2.6GHZ； 3、内存：内存容量≥512GB，类型 DDR4 及以上，频率≥2933MHZ； 4、系统盘：配置≥960GB SSD【2*480GB SSD】硬盘； 5、数据盘：≥46.08TB SSD； 6、网络：配置≥2*双光纤端口 25GE 以太网卡（含光模块）； 7、电源：配置≥2 路热插拔电源，每单路热插拔电源可满足设备满载运

服务器类型	配置
	行要求，任意一路电源故障设备功能应不受影响。
存储Ⅱ型	1、2U 机架式服务器； 2、CPU: 配置≥2 颗安全自主可控 CPU；单颗 CPU 要求：X86 架构核数≥24，主频≥2.2GHZ 或 ARM 架构核数≥32 核，主频≥2.6GHZ； 3、内存：内存容量≥512GB，类型 DDR4 及以上，频率≥2933MHZ； 4、系统盘：配置≥960GB SSD【2*480GB SSD】硬盘； 5、数据盘：配置≥6.4TB SSD+144TB HDD 硬盘； 6、网络：配置≥2*双光纤端口 25GE 以太网卡（含光模块）； 7、电源：配置≥2 路热插拔电源，每单路热插拔电源可满足设备满载运行要求，任意一路电源故障设备功能应不受影响。

7.1.3.4 网络设备技术要求

本项目涉及的网络设备，中标方均应随主设备配置完整、满配的光模块，具体数量及技术选型以贵州电网公司实际需求为准。

注：配置仅作参考，实际网络、安全资源配置以技术选型后配置为准。

7.1.3.4.1 云网络设备配置要求

7.1.3.4.1.1 核心交换机

技术指标	要求
外观	框式交换机，支持 4 槽位，前后通风，设备适合机柜(800mm 宽×1200mm 深×2000mm 高)安装，详细说明产品尺寸。
硬件架构	1.电源、风扇支持 N:1 冗余 2.主控板≥2，交换网板≥6，业务板槽位≥4 3.满足安全自主可控要求，设备芯片采用安全自主可控
端口	支持 10G、40GE 和 100G 接口板
性能要求	1.4 槽位交换容量≥350T，包转发率≥115000M 2.所有端口支持巨帧转发（≥9216bytes） 3.10G、40G 端口支持路由口、路由子接口功能 4.端口支持 LLDP 功能 5.支持 IPv4/V6 双栈
二层功能	1.VLAN≥4K，支持 STP/RSTP/MSTP 2.支持 DHCPrelay，且 server 地址不小于 2 个 3.支持基于端口的广播风暴/组播/未知单播抑制 4.支持 M-LAG 或 vPC 或 DRNI 等跨机箱链路捆绑技术
三层功能	1.支持 IPv4/v6 双栈支持静态路由、OSPFv2/v3、ISIS/v6、BGP/4+等动态路由协议 2.支持 ECMP 3.支持 VRRP

技术指标	要求
VXLAN 特性	1.支持 Vxlan 协议，且支持 BGP EVPN 协议 2.支持 VXLAN over IPv6 3.支持 IPv6 VXLAN over IPv4 4.支持 VxLAN OAM: VxLAN ping, VxLAN tracert
网络管理	1.支持 POAP/Ansible/ZTP 等设备零配置自动化部署功能 2.支持 NETCONF 标准接口 3.支持 SNMP 通过域名方式访问 4.支持 NTP 客户端，支持时区修正，支持基于 IP 和域名访问 sever 5.支持 Console、Telnet 和 SSH2 命令行配置等网管方式 6.支持单物理端口和聚合组本地镜像、远程镜像 7.支持流量统计功能 8.支持多活多归接入，提升接入侧网络可靠性 9.支持 ERSPAN
无损特性	支持 RDMA 和 RoCE（RoCE v1 和 RoCE v2） 支持 RoCE 流量可视：支持对 RoCE 流量 KPI 进行分析
安全服务	1.支持基本 ACL、扩展 ACL、基于时间 ACL 等安全防护技术 2.支持 AAA 认证，并支持用户分级管理和口令保护 3.支持设置 SNMPv3 加密 4.支持远程日志记录，指定记录服务器 IP 地址
配置	主控 1+1 冗余、电源 1+1 冗余、交换网板不少于 4+2 冗余，40G 接口≥72 个，万兆接口≥48 个，满配对应光模块。

7.1.3.4.1.2 接入交换机-25GE

技术指标	要求
外观	设备适合机柜(800mm 宽×1200mm 深×2000mm 高)安装，详细说明产品尺寸。
硬件架构	冗余电源；冗余风扇 满足安全自主可控要求，设备芯片采用安全自主可控
端口	≥48 口 25GE，≥8 口 QSFP40G/100GE
性能要求	1.交换容量≥4Tbps，包转发率≥1800Mpps
	2.支持堆叠（IRF）/VSS，或者跨设备 LACP 聚合、LACP 边缘端口支持三层转发 3.所有端口支持巨帧转发（≥9216bytes） 4.10G、40G 端口支持路由口、路由子接口功能 5.端口支持 LLDP 功能 6.支持 IPv4/V6 双栈
二层功能	1.VLAN≥4K，支持 STP/RSTP/MSTP 2.支持 DHCPrelay，且 server 地址不小于 2 个 3.支持基于端口的广播风暴/组播/未知单播抑制 4.支持 M-LAG 或 vPC 或 DRNI 等跨机箱链路捆绑技术

技术指标	要求
三层功能	1.支持 IPv4/v6 双栈支持静态路由、OSPFv2/v3、ISIS/v6、BGP/4+等动态路由协议 2.支持 ECMP 3.支持 IPv4/v6 三层组播：PIM-DM/SM,IGMP/MLD 4.支持 VRRP
VXLAN 特性	1.支持 Vxlan 协议，且支持 BGP EVPN 协议 2.支持 VXLAN over IPv6 3.支持 IPv6 VXLAN over IPv4 4.支持 VxLAN OAM: VxLAN ping, VxLAN tracert
网络管理	1.支持 POAP/Ansible/ZTP 等设备零配置自动化部署功能 2.支持 NETCONF 标准接口 3.支持 SNMP 通过域名方式访问 4.支持 NTP 客户端，支持时区修正，支持基于 IP 和域名访问 sever 5.支持 Console、Telnet 和 SSH2 命令行配置等网管方式 6.支持单物理端口和聚合组本地镜像、远程镜像 7.支持流量统计功能 8.支持 ERSPAN
无损特性	支持 RDMA 和 RoCE（RoCE v1 和 RoCE v2） 支持 RoCE 流量可视：支持对 RoCE 流量 KPI 进行分析
安全服务	1.支持基本 ACL、扩展 ACL、基于时间 ACL 等安全防护技术 2.支持 AAA 认证，并支持用户分级管理和口令保护 3.支持设置 SNMPv3 加密 4.支持远程日志记录，指定记录服务器 IP 地址
配置	设备包含满配对应光模块

7.1.3.4.1.3 带外管理交换机

技术指标	要求
外观	机架式 1U 交换机，设备适合机柜(800mm 宽×1200mm 深×2000mm 高)安装，详细说明产品尺寸。
硬件架构	冗余电源 满足安全自主可控要求，设备芯片采用安全自主可控
端口	≥48 口千兆电+≥4 个 SFP+万兆光，含满配对应光模块
性能要求	1.交换容量≥600Gbps，包转发率≥200Mpps 2.所有端口支持巨帧转发（≥9216bytes） 3.端口支持 LLDP 功能，且支持配置 TLV 指定 managementip 地址
二层功能	1.VLAN≥4K，支持 STP/RSTP/MSTP 2.支持 DLDP/UDLD 3.支持基于端口的广播风暴/组播/未知单播抑制
三层功能	1.支持静态路由、OSPFv2、ISIS、BGP 等动态路由协议 2.支持 VRRP

技术指标	要求
网络管理	1.支持 SNMPV1/V2/V3，支持 SNMP 通过域名方式进行访问 2.支持管理 VLAN 3.支持 Console、Telnet 和 SSH2 命令行配置等网管方式
安全服务	1.支持基本 ACL、扩展 ACL、基于时间 ACL 等安全防护技术 2.支持 AAA 认证，并支持用户分级管理和口令保护 3.支持设置 SNMPv3 加密 4.支持远程日志记录，指定记录服务器 IP 地址

7.1.3.4.1.4 接入交换机（数据库）-25GE

技术指标	要求
外观	设备适合机柜(800mm 宽×1200mm 深×2000mm 高)安装，详细说明产品尺寸。
硬件架构	冗余电源；冗余风扇 满足安全自主可控要求，设备芯片采用安全自主可控
端口	≥48 口 25GE，≥8 口 QSFP40G/100GE
性能要求	1.交换容量≥8Tbps，包转发率≥2000Mpps 2.支持堆叠（IRF）/VSS，或者跨设备 LACP 聚合、LACP 边缘端口支持三层转发 3.所有端口支持巨帧转发（≥9216bytes） 4.10G、40G 端口支持路由口、路由子接口功能 5.端口支持 LLDP 功能 6.支持 IPv4/V6 双栈
二层功能	1.VLAN≥4K，支持 STP/RSTP/MSTP 2.支持 DHCPrelay，且 server 地址不小于 2 个 3.支持基于端口的广播风暴/组播/未知单播抑制 4. 支持 M-LAG 或 vPC 或 DRNI 等跨机箱链路捆绑技术
三层功能	1.支持 IPv4/v6 双栈支持静态路由、OSPFv2/v3、ISIS/v6、BGP/4+等动态路由协议 2.支持 ECMP 3.支持 IPv4/v6 三层组播：PIM-DM/SM,IGMP/MLD 4.支持 VRRP
VXLAN 特性	1.支持 Vxlan 协议，且支持 BGP EVPN 协议 2.支持 VXLAN over IPv6 3.支持 IPv6 VXLAN over IPv4 4.支持 VxLAN OAM: VxLAN ping, VxLAN tracert
网络管理	1.支持 POAP/Ansible/ZTP 等设备零配置自动化部署功能 2.支持 NETCONF 标准接口 3.支持 SNMP 通过域名方式访问 4.支持 NTP 客户端，支持时区修正，支持基于 IP 和域名访问 sever 5.支持 Console、Telnet 和 SSH2 命令行配置等网管方式

技术指标	要求
	6.支持单物理端口和聚合组本地镜像、远程镜像 7.支持流量统计功能 8.支持 ERSPAN
无损特性	支持 RDMA 和 RoCE（RoCE v1 和 RoCE v2） 支持 RoCE 流量可视：支持对 RoCE 流量 KPI 进行分析
安全服务	1.支持基本 ACL、扩展 ACL、基于时间 ACL 等安全防护技术 2.支持 AAA 认证，并支持用户分级管理和口令保护 3.支持设置 SNMPv3 加密 4.支持远程日志记录，指定记录服务器 IP 地址
配置	设备包含满配对应光模块

7.1.3.4.2 配套网络设备配置要求

7.1.3.4.2.1 汇聚交换机

技术指标	要求
外观	框式交换机，支持 4 槽位，前后通风，设备适合机柜(800mm 宽×1200mm 深×2000mm 高)安装，详细说明产品尺寸。
硬件架构	1.电源、风扇支持 N:1 冗余 2.主控板≥2，交换网板≥6，业务板槽位≥4 3.满足安全自主可控要求，设备芯片采用安全自主可控
端口	支持 10G、40GE 和 100G 线卡
性能要求	1.4 槽位交换容量≥350T，包转发率≥150000M 2.所有端口支持巨帧转发（≥9216bytes） 3.10G、40G 端口支持路由口、路由子接口功能 4.端口支持 LLDP 功能 5.支持 IPv4/V6 双栈
二层功能	1.VLAN≥4K，支持 STP/RSTP/MSTP 2.支持 DHCPrelay，且 server 地址不小于 2 个 3.支持基于端口的广播风暴/组播/未知单播抑制 4. 支持 M-LAG 或 vPC 或 DRNI 等跨机箱链路捆绑技术
三层功能	1.支持 IPv4/v6 双栈支持静态路由、OSPFv2/v3、ISIS/v6、BGP/4+等动态路由协议 2.支持 ECMP 3.支持 VRRP
VXLAN 特性	1.支持 Vxlan 协议，且支持 BGP EVPN 协议 2.支持 VXLAN over IPv6 3.支持 IPv6 VXLAN over IPv4 4.支持 VxLAN OAM: VxLAN ping, VxLAN tracert
网络管理	1.支持 POAP/Ansible/ZTP 等设备零配置自动化部署功能 2.支持 NETCONF 标准接口 3.支持 SNMP 通过域名方式访问

技术指标	要求
	4.支持 NTP 客户端，支持时区修正，支持基于 IP 和域名访问 sever 5.支持 Console、Telnet 和 SSH2 命令行配置等网管方式 6.支持单物理端口和聚合组本地镜像、远程镜像 7.支持流量统计功能 8. 支持 ERSPAN
无损特性	支持 RDMA 和 RoCE（RoCE v1 和 RoCE v2） 支持 RoCE 流量可视：支持对 RoCE 流量 KPI 进行分析
安全服务	1.支持基本 ACL、扩展 ACL、基于时间 ACL 等安全防护技术 2.支持 AAA 认证，并支持用户分级管理和口令保护 3.支持设置 SNMPv3 加密 4.支持远程日志记录，指定记录服务器 IP 地址
配置	主控 1+1 冗余、电源 1+1 冗余、交换网板不少于 4+2 冗余，万兆接口≥48 个，满配对应光模块。

7.1.3.4.2.2 千兆交换机

技术指标	要求
外观	机架式 1U 交换机，前后通风，设备适合机柜(800mm 宽×1200mm 深×2000mm 高)安装，详细说明产品尺寸。
硬件架构	冗余电源；冗余风扇 满足安全自主可控要求，设备芯片采用安全自主可控
端口	≥48 口千兆电+≥4 个 SFP+万兆光，含满配对应光模块
性能要求	1.交换容量≥600Gbps，包转发率≥200Mpps 2.支持堆叠（IRF）/VSS，或者跨设备 LACP 聚合、LACP 边缘端口支持三层转发 3.所有端口支持巨帧转发（≥9216bytes） 4.10G、40G 端口支持路由口、路由子接口功能 5.端口支持 LLDP 功能 6.支持 IPv4/V6 双栈
二层功能	1.VLAN≥4K，支持 STP/RSTP/MSTP 2.支持 DHCPrelay，且 server 地址不小于 2 个 3.支持基于端口的广播风暴/组播/未知单播抑制
三层功能	1.支持 IPv4/v6 双栈支持静态路由、OSPFv2/v3、ISIS/v6、BGP/4+等动态路由协议 2.支持 ECMP 3.支持 IPv4/v6 三层组播：PIM-DM/SM,IGMP/MLD 4.支持 VRRP
网络管理	1.支持 POAP/Ansible/ZTP 等设备零配置自动化部署功能 2.支持 NETCONF 标准接口 3.支持 SNMP 通过域名方式访问 4.支持 NTP 客户端，支持时区修正，支持基于 IP 和域名访问 sever 5.支持 Console、Telnet 和 SSH2 命令行配置等网管方式

技术指标	要求
	6.支持单物理端口和聚合组本地镜像、远程镜像 7.支持流量统计功能
安全服务	1.支持基本 ACL、扩展 ACL、基于时间 ACL 等安全防护技术 2.支持 AAA 认证，并支持用户分级管理和口令保护 3.支持设置 SNMPv3 加密 4.支持远程日志记录，指定记录服务器 IP 地址

7.1.3.5 安全设备参数要求

本项目涉及的安全设备，中标方均应随主设备配置完整、满配的光模块，具体数量及技术选型以贵州电网公司实际需求为准。

7.1.3.5.1 云出口防火墙

类型	指标项	指标要求
设备硬件要求	硬件架构	采用国产芯片，提供第三方测试报告
	操作系统	采用国产操作系统，提供第三方测试报告
	产品形态	1U 或 2U
	硬件规格	CPU 核数≥4，存储容量≥240G SSD，内存≥32G；
	接口数量	■1 个 console 口 ■1 个独立 MGT 接口，1 个独立 HA 接口 ■USB 3.0≥1 个 8 个 GE 电口 4 个 SFP 光口 ■8 个 SFP+光口（接口可通过扩展槽位扩展满足即可）满配对应光模块，万兆口支持自适应千兆。
	扩展槽	≥2 个扩展槽，支持额外扩展 Bypass 插卡（可设备自带接口支持）
	电源规格	实配双冗余交流电源
	热插拔支持	电源模块支持热插拔
性能要求	吞吐量	标配整机吞吐量≥50Gbps；
	最大并发会话数	≥2000 万
	每秒 HTTP 新建连接数	≥50 万
防火墙功能	部署模式	支持透明、路由、混合、旁路四种工作模式
		支持在旁路模式下对流量进行统计、扫描、记录和会话重置
	策略优化	支持对防火墙策略命中次数进行统计、支持防火墙策略冗余检查
		支持基于服务/应用自动生成安全策略
		安全策略支持 IPv6 报文头部检查
	NAT 功能	支持一对一，一对多，多对多等多种 NAT 转换模

类型	指标项	指标要求
		式
		支持命中数分析，显示命中数、首次命中时间、最近一次命中时间、未命中天数等信息，并可针对分析结果，对 NAT 条目进行删除或禁用
		支持 NAT 配置导出
	通配符掩码	地址簿支持配置通配符子网掩码，并支持配置排除地址成员
	长连接功能	支持自定义长连接功能
	支持 DNS-rewrite 功能	防火墙支持 DNS-rewrite 功能，生成映射关系，并修改 DNS 响应报文中的域名对应的 IP 地址，以隐藏和保护域名对应的服务器真实 IP 地址
	TCP 处理机制	TCP 三次握手建立阶段与四次握手关闭阶段各个超时时间可自定义，通过 TCP 处理机制自定义可提高对业务系统的兼容性和稳定性。
	监控	支持监控设备系统资源的实时状况，包括 CPU/内存状态、会话数、接口流量等对象
		支持设备、接口的流量统计将 IPv6 和 IPv4 分开统计呈现
		支持通过 netflow 进行流量信息采集和外发
		支持链路状态监控，包括延时、丢包率、抖动
	报警	支持针对 CPU 利用率、内存利用率、接口带宽、会话资源、SNAT 转换端口资源等进行监控告警
		支持日志、SNMP Trap 报文报警方式
	ALG 应用	支持所列所有应用，包括：H.323、SIP、FTP、TFTP、RSH、RTSP、SQLNetV2、HTTP、MS-RPC、PPTP、SUN-RPC
	PTF	PTF 支持 IP 外部动态列表
负载均衡	智能链路负载均衡	支持智能链路负载均衡技术，可实时探测链路质量，动态调整链路转发比重，使流量在最优链路进行转发
	多链路负载均衡	支持基于源、基于源和目的、基于会话等多种负载均衡模式
	服务器负载均衡	支持服务器健康检查和会话保持功能，支持加权轮询、加权最小连接数、加权散列等多种服务器负载均衡算法
	支 持 SmartDNS 功能	使外网访问内部服务器的流量可以在多条链路上实现智能分担
路由协议	路由协议	支持 IPv4 和 IPv6 的静态路由
		支持 OSPF、BGP、ISIS 和 RIP、支持策略路由、支持 ISP 路由并内置多运营商 ISP 信息
		支持组播 PIM-SSM、PIM-SM 路由协议
		支持 OSPFv3、BGP4+、IPv6 ISIS、RIPng 等 IPV6 动态路由协议

类型	指标项	指标要求
		支持基于应用的策略路由，可将 P2P 应用引流到低价值链路上，提升链路的利用率和用户的服务质量
VPN	IPsec VPN	支持 IPSEC VPN 配置向导功能
高可靠性（HA）	高可靠性（HA）	支持 A-P 模式，支持 A-A 模式，支持非对称路由场景
		支持命令行进行主备切换
		支持基于接口、HTTP、ICMP、ARP、DNS、TCP 等监测对象实现主备切换
		支持两组 HA 设备组成 Twin-mode HA
SSL 代理	SSL 解密	支持 IP 白名单功能
		支持内置网站白名单功能
攻击防护	抗 DDoS 攻击	支持抵御所列所有攻击类型，包括：DNS Query Flood、SYN Flood、UDP Flood、ICMP Flood、Ping of Death、Smurf、Winnuke
		抗攻击模块可以只告警不进行丢弃
	会话控制	支持会话控制功能，要求能够基于源/目的、应用、协议、角色/用户、时间表五种条件做会话数限制
		支持会话控制功能，要求能够限制最大会话连接数与会话新建速率
入侵防御	入侵防御	支持 IPS 入侵防御规则库，支持针对 HTTP、SMTP、IMAP、POP3、VOIP、NETBIOS 等 20 余种协议和应用的攻击检测和防御，具备超过 12000 种特征库规则，特征库规则列表至少支持基于协议类型、操作系统、攻击类型、严重程度、特征 ID 等方式的查询，支持 IPS 库在线/离线升级
		支持 SQL 注入、XSS 防护，支持 URL、Cookie、Referer、Post 检查点
		支持外链检查防护，支持自定义外链特性，类型支持 HTTP、HTTPS、FTP
		支持 CC 攻击检测，支持访问限速、代理限速、自定义请求阈值、爬虫友好等方法，检测到 CC 攻击时支持 JS Cookie、重定向、访问确认、验证码四种认证方法
病毒防护	扫描文件类型	支持对 HTTP、FTP、SMTP、POP3、IMAP 协议的应用进行病毒扫描和过滤
	压缩文件扫描	支持对压缩文件类型的病毒检测，且不小于 5 层压缩，支持对超出行为自定义处理方式。
	防病毒及恶意网站	支持发现恶意软件和恶意站点的警告提示，提示用户所访问的网站为恶意站点或者发现病毒
	特征库数量及升级	支持超过 500 万的病毒特征库，支持病毒库在线/离线升级

类型	指标项	指标要求
数据安全	内容过滤	内容过滤支持预定义关键字及文件内容过滤
带宽管理	带宽管理	支持 QoS 功能，支持根据安全域、接口、地址、用户/用户组、服务/服务组、应用/应用组、TOS、Vlan 等信息划分管道
		支持两层八级管道嵌套，能够同时做到两个维度的流量控制，支持针对每 IP 或每用户配置最大带宽和最小带宽
		支持针对每 IP 或每用户进行延迟限速
网页访问控制	网页访问控制	支持自定义 URL 类别
		支持 30 万本地 URL 特征库，URL 库支持网络定时更新
管理功能	配置备份	支持自动备份配置文件到 FTP、TFTP 服务器
	日志	支持日志分级，并在日志输出时提供明确的等级标识
		支持 URL 日志、NAT 日志、会话日志、威胁日志等多种日志类型，可分别开启或关闭日志记录
		支持基于标准 SYSLOG 以及二进制的日志两种格式；支持分布式存储到多台日志服务器，分布的算法至少支持轮询方式、源 IP HASH 方式
	SNMP	支持 SNMPV1/V2C/V3 三种版本
		支持查询 CPU 利用率、内存利用率、新建连接速率、系统支持的最大会话数、接口的入方向速率和出方向速率、设备 HA 状态等
	分级管理	支持分级权限管理功能，为用户提供不同级别的管理权限，支持自定义管理员角色
开放	API	支持 Restful API
	Netconf	支持 Netconf
资质要求	销售许可	具备以下任意条件之一： 1. 具有安全认证合格证明材料或者符合《信息安全技术网络安全专用产品安全技术要求》强制要求的证明材料，证明材料须由《承担网络关键设备和网络安全专用产品安全认证和安全检测任务机构名录》相关机构出具。 2. 具备有效期内的国家安全产品销售许可。
	第三方性能检测报告	需提供第三方性能测试报告

7.1.3.5.2 边界防火墙

类别	功能与技术描述

类别	功能与技术描述
硬件平台	1U 或 2U 机架，实际配置可插拔冗余电源；满足安全自主可控品牌要求，要求采用安全自主可控主处理芯片、操作系统，具备完整自主知识产权；必须独立专业防火墙设备，非插卡式扩展的防火墙设备。
硬件规格	CPU 核数≥4，存储容量≥1T SSD，内存≥64G；实际配置千兆电接口≥8，千兆光接口≥4，万兆光接口≥8，扩展槽数量≥2；支持额外扩展 Bypass 插卡（可设备自带接口支持）满配对应光模块；
性能要求	防火墙吞吐量（最大）≥30Gbps；IPS 吞吐量（最大）≥12Gbps；防病毒吞吐量（最大）≥18Gbps；最大并发连接数≥2000 万；每秒新建连接数（最大）≥50 万；IPSEC 吞吐量（最大）≥2.8Gbps；SSL VPN 用户数（最大）≥4000
访问控制	支持基于 IPV4/IPV6 的接口/安全域、地址、用户、服务、应用和时间的防火墙访问控制策略，
	支持基于 IPV4/IPV6 的接口/安全域、地址、用户、服务、应用和时间的会话控制策略，包括总连接数控制、每秒总新建连接数控制、每 IP 总连接数控制、每 IP 新建连接数控制。
入侵防御	支持并开通网络入侵检测及防御功能，入侵防御事件库事件数量不少于 12000 条
	可基于 IP 地址、网段、用户、时间、VLAN、协议类型等条件设定入侵防御模块的检测事件及响应方式。
	提供 SQL 注入攻击、XSS 攻击的检测和防御功能，对 Web 服务系统提供保护；
防病毒	支持并开通对 HTTP、FTP、SMTP、POP3、IMAP 协议的病毒检测和过滤功能；
	基于主流杀毒引擎，支持对文件感染型病毒、蠕虫病毒、脚本病毒、宏病毒、木马、恶意软件等过滤
	支持 10 层以上压缩文件
	防病毒功能开启后，整机处理性能衰减不超过 30%
威胁情报	支持本地离线库在线更新，离线更新。
	支持失陷检测情报分类：勒索软件、挖矿软件、网银木马、窃密木马、黑客工具、后门软件、僵尸网络、常规木马、矿池数据、APT 攻击及其他远控等风险流量进行识别和过滤。可对不同类别风险 IP 流量进行记录日志或者阻断一定时间。
安全检测	支持联动云端威胁情报中心， 可通过云端安全检查系统进行攻击识别，识别的攻击类型应至少包含：后门、远控木马、DDOS、挖矿、银行木马、APT、DGA、黑客工具、勒索软件、数据窃取、蠕虫、钓鱼网站、黄赌毒等威胁。
WAF 能力	支持 WEB 防护功能，支持对 100 个站点制订 Web 应用防护策略
	支持自定义 WEB 安全防护事件，可对 HTTP 请求回应的头、体检查；
	支持自定义 WEB 安全防护事件，可以对请求参数、各个头域、内容关键字、文件类型等进行灵活组合生成策略。
弱口令	支持弱口令密码检查
行为管理及流量控制	支持并开通基于 DPI 和 DFI 技术的应用特征识别及行为控制，应用识别的种类不少于 5000 种；支持并开通基于 URL 分类库的 WEB 访问管理，URL 分类库规模不少于 2000 万条

类别	功能与技术描述
VPN	支持并开通 IPSec VPN、GRE VPN，并且支持从管控平台查询到每条 ipsec 隧道、gre 隧道的实时包、抖动、延迟数据以图形化界面进行展示
	支持并开通 SSL VPN，支持本地密码认证、口令认证、第三方对接认证、证书认证等认证方式。
	支持多台防火墙设备在管控平台进行 2 种及以上的 vpn 隧道的配置和管理，并实时上报 vpn 隧道状态在控制平台以图形化界面进行展示。
国密	支持加密卡或软件方式，支持 SM2，SM3，SM4 国密算法。
网络特性	支持 VXLAN 功能，支持跨局域网络建立二层转发
DNS	支持标准 DNS 服务器功能，支持多种 DNS 记录 ，包括不限于 A ，AAA，PTR 记录
	支持 DNS 透明代理功能，可将指定范围内的 DNS 请求自动重定向至管理员指定的 DNS 服务器，且支持多台 DNS 服务器的负载均衡。
系统管理	支持设备 web 页面抓包功能，支持基于接口，协议、地址类型（ipv4/ipv6）、客户端到防火墙、防火墙到目的服务器以及全部流量的匹配方式进行抓包；支持基于接口的入流量、出流量、双向流量的接口镜像功能，
	支持基于并发会话数量的 TOP100 用户的展示数据和 TOP10 应用的并发数量曲线图，并发数量曲线图的统计周期包括小时、天、7 天和 30 天。
	WEB 界面的网络调试功能，支持 PING、TRACEROUTE、TCP 探测方式，支持模拟数据流穿过设备时各个功能模块处理流程以及结果进行展示。

7.1.3.5.3 运维区防火墙

类别	功能与技术描述
安全认证	满足国家安全产品有关认证要求。
产品架构	基于自主可控芯片的多核 CPU 架构
系统安全性	采用防火墙专用操作系统
	支撑系统不提供多余的网络服务
	系统不含任何高、中风险安全漏洞
冗余电源	提供双电源供电，并支持故障告警
设备支撑	配置设备机箱配套支架，设备高度不大于 2U
端口数量及类型	业务口要求：提供 2 个万兆光接口、8 个千兆光接口用于网络通讯，提供管理接口和 HA 端口。满配对应光模块
整机吞吐量	数据包吞吐量≥15Gbps
最大并发连接数	最大并发连接数≥300 万
每秒新建连接数	每秒新建连接数≥10 万
静态路由	最大静态路由条数≥1000 条
	支持基于源、目的 IP 地址的策略路由能力
访问控制策略	最大访问控制策略条数≥10000 条、最大地址集建立数目≥30000 条、最大服务集建立数目≥30000 条，最大域名对象数目≥3000 条
工作模式	1.支持透明模式
	2.支持路由模式
	3.支持混合模式

协议支持	1.支持 TCP、UDP 协议
	2.支持 IPv4、IPv6、ICMP、GRE（无需绑定物理接口）、VRRP、OSPF、BGP、RIP、SNMP 等协议
	3.支持 ARP、VLAN Trunk、QinQ 等协议
链路捆绑	1.支持多条链路的捆绑及链路间的负载均衡
NAT 功能	1.支持静态网络地址转换(Static NAT)
	2.支持动态网络地址转换(Dynamic NAT)
	3.支持网络地址及端口转换(PAT)
ALG 功能	1.能够识别常见应用协议并进行应用层处理
	2.支持对动态端口协议进行识别并控制
状态监测	1.支持基于会话的安全过滤，根据会话表放行或阻断数据包
	2.支持会话管理表，能够对特定的会话直接操作（删除等）
	3.支持会话超时保护，无报文的会话在一定时间后自动删除
流量及带宽管理	1.支持对 IP、IP 组、协议及端口进行带宽控制
	2.支持对最大与最小带宽进行限制
	3.支持根据 IP 地址限制并发 session 数量
连接控制	1、支持对源/目的地址对象、应用等设置并发和新建会话数量
	2、支持展示被拦截的 IP、地址对象、被拒次数、最近被拒时 间等信息
策略优化	1.支持分析失效、冗余、冲突的策略
	2.支持对策略有效性进行统计，支持策略的命中统计
	3.支持策略查询及导出功能
	4.支持批量修改策略配置信息，如批量禁用策略、批量删除 策略等
IPV6 功能	1.支持 IPv6 协议栈，支持 IPv6 地址的正确解析
	2.支持 IPV6 的 ACL 过滤
	3.支持 IPv6 的路由协议，包括 IPv6 的静态路由、动态路由（含 OSPFv3）和策略路由
	4.支持 IPV6 的状态检测功能
	5.支持 IPV6 的报文检测功能
	6.支持 NAT64、IPv4/IPv6 双栈
	7 支持 IPV6 DDOS 等攻击防护功能
	8.设备纯 IPv4 及纯 IPv6 的性能要求一致
攻击防御	1.支持对常见攻击方式进行检测与防御（DDOS、特殊报文、扫描攻击、特殊控制报文攻击等）
	2.抵抗各种典型的拒绝服务攻击，包括 SYN FLOOD，UDP FLOOD，ICMP FLOOD，IP 碎片包攻击，源 IP 地址欺骗攻击
	3.支持数据包的深度检测
	4.支持基于源及目的 IP 地址的并发连接数的控制
访问控制	1.支持基于域名的访问控制，且无需改变主机、终端的域名解 析配置
	2.支持基于 IP 地址的访问控制
	3.支持基于端口的访问控制
	4.支持基于协议的访问控制
	5.支持基于时间的访问控制
	6.支持基于连接的访问控制

	7.支持默认禁止策略
	8.支持用户自定义安全策略
黑白名	1.支持黑名单功能，被列入黑名单的 ip 及 ip 地址段，禁止所有访问，支持有效期设置，并提供黑名单增删 api 接口；黑名 单条码不少于 3000 条；
	2.支持白名单功能，被列入白名单的 ip 及 ip 地址段，放行所有访问，支持有效期设置，并提供白名单增删 api 接口；
IPSEC VPN	1.支持 IPSEC VPN。支持对隧道内流量进行监控
	2.支持多种（国际、国内）加密算法
应用控制	1．支持识别并控制各种常见应用
	2.支持自定义应用特征
入侵防御	1.支持告警和拦截非法、不正常、含攻击行为的报文
	2.支持手动自定义攻击规则库
	3.支持在线、离线、手动升级规则库
	4.至少支持威胁阻断模式、威胁监测模式
URL 过滤	1.支持黑白名单、恶意 URL 过滤
	2.内置恶意 URL 库，并支持在线、离线、手动更新
	3.支持自定义 URL 和阻断界面内容
	4．支持 URL 通配符，可通过通配符阻断某网站二级网站或页面
病毒过滤	1.支持对数据报文及文件进行病毒查杀
	2.支持对病毒报文及文件进行查杀、隔离等操作
	3.可拦截典型木马攻击行为
	4.支持在线、离线、手动更新规则库
管理方式	1.支持本地串口管理、远程管理、集中管理、分级管理等
	2.支持多主控台同时管理
	3.支持 HTTPS，SSH 等管理方式
	4.支持设置、查询和修改安全策略
	5.支持鉴别失败管理
	6.支持设备及策略集中管理
系统管理	1.支持自身状态监控，支持 snmp 管理，支持流量监测，提供支持设备状态监控、流量监控的北向 api 接口
	2.支持带外网管接口
	3.支持 Trap 协议
	4.支持配置备份、NTP 时间同步等
用户管理	1.支持对授权管理员的口令鉴别方式
	2.支持管理员权限划分
	3.支持对授权管理员、主机和用户进行身份鉴别
日志管理	1.支持流量日志、事件类日志、操作类日志、运行类日志及用户日志
	2.支持本地日志导出、日志清空、日志查询等
	3.支持 SYSlog 等方式发送至多个日志服务器，提供 syslog 范式化服务
	4.支持设置日志传输参数
行为审计	1.支持用户行为审计
	2.支持审计数据查询

自身安全性	1.支持配置限定用户登陆的 IP 地址范围
	2.支持 SSH、HTTPS 等加密方式进行远程访问
	3.支持对用户口令进行加密保存
	4.支持用户口令复杂度设置及检查
	5.支持最大登录失败重试次数设置
	6.支持用户登录超时时间设置
	7.支持双因子认证方式
	8.应保证所用的操作系统不存在安全漏洞
对外接口	1.设备应具备开放性、可扩展性，并提供开放接口，其中对外接口包括：允许策略增删改查、特征库版本、运行状态、策略命中情况等信息
	2.支持通过 SYSlog 方式以 UDP 发送日志对接监测系统，并可配合完成联动测试
可靠性与可用性	1.应提供 MTBF(Mean Time Between Failure)和 MTTR(Mean Time To Repair)指标，其中 MTBF 不小于 5 万小时，MTTR 不大于 2 小时
	2.支持电源冗余，电源冗余单元应支持热插拔功能
	3.支持软件防护加载、升级失败回滚
	4.支持 trouble-shooting 和性能监控、故障跟踪能力
	5.支持双机备份（双机热备、双机冷备）功能
	6.支持双机配置同步功能
	7.支持主备切换会话保持
	8.支持在关闭防火墙策略时，能够正常路由转发数据包
	9.支持设备状态监测、端口状态监测、链路连通性状态监测，可根据监测的设备状态，实现秒级的高可用切换，保障业务连续性
	10.应具有软件故障的监视功能，一旦软件出现死循环等重大故障时，应能自动再启动，并作出即时故障报告信息
供应链稳定性	具备供应链稳定性
售后服务	整机软硬件 5 年免费原厂维护、管理软件升级维护及技术支持服务（含特征库、规则库、许可等各种软件限制性的授权服务）

7.1.3.5.4 堡垒机

指标项	具体要求
兼容性	1、产品及其依赖项满足《GB/T 36572-2018 电力监控系统网络安全防护导则》相关要求，应实现自身的安全，应安全、可控、可靠。 2、产品及其依赖项满足《GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求》3 级。
本体安全	1、产品及其依赖项满足《GB/T 36572-2018 电力监控系统网络安全防护导则》相关要求，应实现自身的安全，应安全、可控、可靠。 2、产品及其依赖项满足《GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求》3 级。 3、远程管理设备时，应建立安全的通信协议。

指标项	具体要求
授权要求	支持≧1500 个资产。
硬件规格	1、CPU 核数≥8，内存≥32GB，存储≥4T。 2、网络接口，配置≧（2 千兆电口+2 万兆光口），以上光模块满配.支持 ipv4 和 ipv6 双协议栈。 3、设备尺寸≤2U 标准机箱。
安全及管理	1、配置国密密码卡，实现通信数据的机密性和完整性；实现访问控制信息和日志记录的完整性保护；计量自动化系统为等保三级系统，国密密码卡应符合《GM/T0028 密码模块安全技术要求》安全二级及以上要求。 2、配置国密 USB Key 数量≥30，USB Key 需要满足本次招标的智能密码钥匙技术参数。 3、配置 CA 机构个人数字证书 10 套≥5 年授权。 4、支持审计日志自动、手动备份。日志最少保留 6 个月。 5、支持标准 SNMP 管理协议，支持 syslog 等标准日志格式外发。 6、实时监控系统 CPU、内存、磁盘的使用情况，支持 CPU、内存、磁盘使用超过阈值告警。
部署能力	1、支持 IPv6、IPv4 双协议栈。 2、物理旁路单臂部署，以逻辑网关方式工作；不改变现有网络结构。 3、单机部署、双机热备（HA）部署、分布式部署。 4、支持 B/S 运维。 5、支持 SNMP 协议：可对外提供终端设备的 CPU 利用率，内存利用率，磁盘空间利用率、网络等信息，支持 SNMP trap 告警外发；支持 Syslog 协议外发日志。
支持协议	1、字符协议：SSHv1、SSHv2、TELNET。 2、图形协议：RDP、VNC。 3、文件传输协议：FTP、SFTP、RDP 磁盘映射、RDP 剪切板。 4、协议代理审计模块：部署于 Liunx 服务器上，用于发布非标准协议或应用客户端并进行审计。
分权分域	1、系统内置系统管理员、审计管理员、安全管理员。 2、系统管理员可针对不同用户指定不同的管理权限，可设定用户（组）和资源（组）的管理范围。
用户管理	1、用户登录认证方式支持静态口令认证、手机动态口令认证、USB Key（数字证书）认证、AD 域认证、Radius 认证等认证方式；并支持各种认证方式和静态口令组合认证。 2、支持批量导入、导出用户信息。 3、支持用户手动添加、删除、编辑、设定角色、单独指定登录认证方式、设定用户有效期。 4、支持对用户指定限制登录 IP、登录时间段等规则。 5、支持口令有效期设置，用户账号口令到期强制用户修改自身口令。 6、支持登录控制台会话超时时间设置，用户在指定时间内无操作自动注销当前会话。 7、支持设定访问锁定策略，达到限制主账号密码输入错误次数和锁定时间的目的。
资源管理	1、支持服务器资源、网络设备资源、数据库资源、安全设备资源、C/S 资源、B/S 资源。

指标项	具体要求
	2、支持“内置应用发布服务器功能”；或针对 C/S 架构的资产管理，需要单独配置外置应用发布服务器。 3、支持批量导入导出资源；支持手动添加、删除、编辑、查询资源。 4、支持资源的单点登录。
运维授权	1、支持一对一、一对多、多对多授权，如将单个资产授权多个用户，一个用户授予多个资产，用户组向资产组授权。 2、支持按授权名称、用户名称、用户账号、资源名称、资源地址、资源账号查询已授权信息。 3、支持在授权基础上设定双人复核登录，登录时必须经过第二人授权后才能登录。
账号托管	1、支持定期变更目标设备真实口令。 2、支持密码策略设置。
审计日志	1、支持监控正在运维的会话，信息包括运维用户、运维客户端地址、资源地址、协议、开始时间等并可以实时阻断（支持命令黑名单和命令审批规则）。 2、对字符命令方式的访问可以审计到所有交互内容，可以还原操作过程的命令输入和结果输出。 3、图形资源访问时，支持键盘、剪切板、窗口标题、文件传输记录，并且对图形资源的审计回放时。 4、自定义审计查询条件，包括：时间范围、用户与用户 IP、资源 IP、命令关键字条件。 5、提供用户统计报表和系统运行报表并支持导出。

7.1.3.5.5 网络终端接入核查设备

指标项	具体要求
兼容性	1、产品及其依赖项满足《GB/T 36572-2018 电力监控系统网络安全防护导则》相关要求，应实现自身的安全，应安全、可控、可靠。 2、产品及其依赖项满足《GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求》3 级。
本体安全	1、产品及其依赖项满足《GB/T 36572-2018 电力监控系统网络安全防护导则》相关要求，应实现自身的安全，应安全、可控、可靠。 2、产品及其依赖项满足《GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求》3 级。 3、可限制仅特定地址登录。 4、远程管理设备时，应建立安全的通信协议。
授权要求	支持≧1500 个终端数。
硬件要求	1、CPU 核数≧8；内存大小：≧32G，硬盘容量：≧960G。 2、配置冗余电源。 3、网络接口，配置≧（2 千兆电口+2 万兆光口），以上模块满配。支持 ipv4 和 ipv6 双协议栈。 4、设备外形及安装：2U 及以下标准机架。

指标项	具体要求
功能要求	实现以下功能的产品及其依赖项，均为本产品的供货范围： 1、支持扫描识别网络内的终端设备及类型并展示。 2、支持 802.1X：在网络接入层做准入认证、根据认证授权情况确定是否能访问网络。 3、支持 Portal：当新终端接入交换机时，交换机发现该终端未经身份认证，则将其浏览器请求重定向至 Portal 认证页面，用户通过身份认证成功后即可正常访问网络。 4、支持 MAB：启用此特性后，当通过 802.1X 认证的端口连接的设备是无法进行交互认证的设备时，交换机就会尝试使用基于 Mac 地址的免认证特性来识别客户端。 5、支持 SNMP 协议：可对外提供终端设备的 CPU 利用率，内存利用率，磁盘空间利用率、网络流量使用信息等信息，支持 SNMP trap 告警外发；支持 Syslog 协议外发日志。

7.1.3.5.6 万兆正向隔离装置

类别	功能与技术描述
总体需求	万兆物理隔离；
	机架式安装，含机架安装套件；
	具备电力专用安全防护设备的检测证明；
	具备公安部颁发的《计算机信息系统安全专用产品检测证书》；
	应通过有关部门组织的电磁兼容性检测；
	采用非 Intel 指令系统（及兼容）的 RISC 微处理器构筑内外网隔离系统；
	嵌入式安全操作系统，去除不需要的所有系统服务；
功能要求	本身应能够一定程度防御常见的网络攻击，包括 ARP Attack、Ping Attack、Ping of Death Attack、Smurf Attack、Unreachable Host Attack、Land Attack、Teardrop Attack、Syn Attack 等；
	数据单向传输，1bit 返回信息；
	表示层与应用层数据完全单向传输，即从安全区 III 到安全区 I/II 的 TCP 应答禁止携带应用数据；
	透明工作方式：虚拟主机 IP 地址、隐藏 MAC 地址；
	基于 MAC、IP、传输协议、传输端口及通信方向的综合报文过滤与访问控制；
	支持 NAT；
	隔离设备的关键芯片和元器件都进行产品老化试验，所有的隔离设备在出厂前必须经过不少于 72 小时连续通电测试，并提供相关质量报告；
	防止穿透性 TCP、UDP 连接；
	配置冗余电源，支持双机热备；
	支持“单进单出”“双进单出”“双进双出”等多种连接方式；
	支持系统告警，支持完备的安全事件告警机制，当发生非法入侵、装置异常、通信中断或丢失应用数据时，可通过网络向第三方日志告警管理系统输出报警信息，日志格式遵循 Syslog 标准；

类别	功能与技术描述
	维护管理方便、安全：基于证书的管理人员认证，图形化的管理界面；
性能要求	CPU 主频≥1.8GHz；
	CPU 核心≥12 核；
	万兆状态下数据传输率≥5Gbps；
	最大并发联接数≥10000；
	数据包转发延迟＜1ms（90%吞吐量）；
	满负荷数据包丢弃率为 0%（90%吞吐量）；
	内网网络接口：至少包含 4 个 GE 业务接口、4 个 SPF+接口，1 个 GE 管理接口，1 个 RS232、1 个 USB 口，网络速率自适应，满配的光模块；
	外网网络接口：至少包含 4 个 GE 业务接口、4 个 SPF+接口，1 个 GE 管理接口，1 个 RS232、1 个 USB 口，网络速率自适应，满配的光模块；
	平均无故障时间＞60000 小时（100％负荷）；
质保要求	含五年原厂保修和软件升级。

7.1.3.5.7 万兆反向隔离装置

类别	功能与技术描述
总体需求	万兆物理隔离；
	机架式安装，含机架安装套件；
	具备电力专用安全防护设备的检测证明
	具备公安部颁发的《计算机信息系统安全专用产品检测证书》；
	具备国家密码管理局商用密码检测中心颁发的《商用密码产品认证证书》
	应通过有关部门组织的电磁兼容性检测；
	采用非 Intel 指令系统（及兼容）的 RISC 微处理器构筑内外网隔离系统；
	配置本设备用加密卡，并配套提供对侧接口服务器用加密卡，以提升传输过程中的加密性能。
	嵌入式安全操作系统，去除不需要的所有系统服务；
功能要求	本身应能够一定程度防御常见的网络攻击，包括 ARP Attack、Ping Attack、Ping of Death Attack、Smurf Attack、Unreachable Host Attack、Land Attack、Teardrop Attack、Syn Attack 等；
	具有基于数字证书的数据签名/解签名功能，具有电力加密算法进行数字加密功能；
	具有应用数据内容有效性检查功能；
	具有 E 文本编码检查功能；
	实现两个安全区之间的非网络方式的安全的数据传递；
	透明工作方式：虚拟主机 IP 地址、隐藏 MAC 地址；
	支持 NAT；
	基于 MAC、IP、传输协议、传输端口及通信方向的综合报文过滤与访问控制；
	防止穿透性 UDP 联接；
	数据单向传输，1bit 返回信息；

类别	功能与技术描述
	配置冗余电源，支持多机阵列；
	支持“单进单出”“双进单出”“双进双出”等多种连接方式；
	支持系统告警，支持完备的安全事件告警机制，当发生非法入侵、装置异常、通信中断或丢失应用数据时，可通过网络向第三方日志告警管理系统输出报警信息，日志格式遵循 Syslog 标准；
	内网网络接口：至少包含 4 个 GE 业务接口、4 个 SPF+接口，1 个 GE 管理接口，1 个 RS232、1 个 USB 口，网络速率自适应，满配的光模块；
	外网网络接口：至少包含 4 个 GE 业务接口、4 个 SPF+接口，1 个 GE 管理接口，1 个 RS232、1 个 USB 口，网络速率自适应，满配的光模块；
	维护管理方便、安全：基于证书的管理人员认证，图形化的管理界面。
性能要求	CPU 主频≥1.8GHz；
	CPU 核心≥12 核；
	密文有效网络吞吐率≥4Gbps；
	数字签名速率≥30000 次/秒；
	最大并发连接数≥10000；
	数据包转发延迟＜1ms（90%吞吐量）；
	满负荷数据包丢弃率为 0%（90%吞吐量）；
	平均无故障时间＞60000 小时（100%负荷）；
质保要求	含五年原厂保修和软件升级。

7.1.3.5.8 入侵防御设备

指标项	具体要求
兼容性	1、产品及其依赖项满足《GB/T 36572-2018 电力监控系统网络安全防护导则》相关要求，应实现自身的安全，应安全、可控、可靠。 2、产品及其依赖项满足《GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求》3 级。
本体安全	1、产品及其依赖项满足《GB/T 36572-2018 电力监控系统网络安全防护导则》相关要求，应实现自身的安全，应安全、可控、可靠。 2、产品及其依赖项满足《GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求》3 级。 3、可限制仅特定地址登录。 4、远程管理设备时，应建立安全的通信协议。
硬件要求	硬件参数：规格：≤2U，CPU 核数：≧16，内存大小：≧32G，硬盘容量：≧1T，电源：冗余电源，接口：4 千兆电口+6 万兆光口，以上模块满配，支持 ipv4 和 ipv6 双协议栈。
功能要求	实现以下功能的产品及其依赖项，均为本产品的供货范围。 1、支持上传、下载、双向的文件内容过滤。 2、可准确地发现包括钓鱼攻击、恶意 SSL 证书、重定向攻击、获取权限、拒绝服务、漏洞利用等网络攻击行为。 3、提供统计分析面板，可将展示威胁统计、恶意 URL、恶意域名、恶意地

指标项	具体要求
	址内容展示；并支持多时间维度筛选。 4、可在单条策略中启用病毒防护、入侵防御、网址过滤、文件过滤、文件内容过滤、终端过滤等安全功能选项。 5、支持安全策略的快速检索及基于名称、地址多维度的高级策略检索。 6、支持添加报表任务。生成可查看报表。 7、支持离线实现 IPS 特征库、威胁库更新。 8、访问控制规则支持模拟策略匹配，输入源目的 IP、端口、协议五元组信息，模拟策略匹配方式，给出最可能的匹配结果，方便排查故障，或环境部署前的调试。 9、支持针对 HTTP、FTP 协议内容检测与病毒查杀。 10、设备具备独立的入侵防护漏洞规则特征库。 11、设备具备独立的热门威胁库，防护类型包括木马远控、恶意脚本、勒索病毒、僵尸网络、挖矿病毒等。 12、支持本地威胁情报检测和威胁情报库离线升级。 13 安全策略支持基于源安全域、目的安全域、源用户、源地址/地区、目的地址/地区、VLAN 等多种方式进行访问控制。 14、支持 SNMP 协议：可对外提供终端设备的 CPU 利用率，内存利用率，磁盘空间利用率、网络流量使用信息等信息，支持 SNMP trap 告警外发；支持 Syslog 协议外发自身日志。
性能要求	整机吞吐量>=10G； IPS 吞吐>=3G； 最大并发连接数不小于 200 万； 新建连接不小于 10 万/秒。

7.1.3.5.9 费控密码机

技术指标		指标参数
硬件设备	物理端口	标准机架式设备，应可放入 19 英寸标准机架，应至少包含以下端口： 电源端口、密码服务以太网端口、管理以太网端口、管理串口、打印口、密钥销毁触发装置。
	随机数发生器	随机数产生器应采用国家密码管理局批准使用的多片多路物理噪声源芯片
	可靠性	平均无故障工作时间应不低于 30，000 小时
	并发访问	>=2048
功能、性能、安全等要求	初始化功能	密码机应具备初始化功能，实现设备的原始状态到工作状态的转换。初始化操作应 至少包括设置设备主密钥、制作开机安全介质、制作授权安全介质、制作备份安全介质、设置设备参数、设置授权。 XX 密码机的初始化，除必须由厂商进行的操作外，系统配置、密钥管理、管理员管理等关键安全操作均应由用户方设备管理人员完成，密码机应提供图形化界面专用管理软件。

技术指标		指标参数
	密码运算	密码机应配用国家密码管理局认可的密码算法 SM1、SM2、SM3、SM4，采用硬件实现 SM1、SM2、SM3 和 SM4 算法。 SM1 算法加解密速率≥150Mbps SM2 算法签名速率≥6000 次/秒 SM2 算法验签速率≥4000 次/秒 SM3 算法运算速率≥700Mbps SM4 算法加解密速率≥700Mbps
	对称密码算法	密码机应配有 SM1 对称密码算法和 SM4 对称密码算法，SM1 密码算法的实现使用国家密码管理局指定的密码算法芯片，SM4 密码算法的实现遵循 GM/T0002-2012。 对称密码算法的工作模式应至少包括 ECB、CBC、CFB 和 OFB 四种模式。
	公钥密码算法	密码机应配用 SM2 非对称密码算法，SM2 密码算法的实现遵循 GM/T0003-2012。
	密码杂凑算法	密码机应配用 SM3 杂凑算法，SM3 杂凑算法的实现遵循 GM/T0004-2012。另外，SM2 密码算法用于数字签名验签和计算消息认证码时，算法要求配用 SM3 杂凑算法，在 SM2 密码算法中使用的 SM3 杂凑算法的实现遵循 GM/T0004-2012。
	密钥管理	密码机应具备完整的密钥管理机制，密钥保护涵盖密钥的产生、注入、导入/导出、备份/恢复、查询和销毁整个生命周期，密码机必须保证密钥在生存周期的各个环节的安全性。密钥安全风险是指业务系统中的各种主控密钥和应用密钥在分发、保存、使用中的泄露、篡改、非法替换的风险。密码机应提供密钥安全性的设计保障。安全性设计应有明确的密钥保护措施和方法来消除密钥安全风险。
	访问控制	密码机应提供访问控制功能，防止非授权访问密码机引起的安全风险。访问控制包括密码机的管理、使用和业务等方面内容
	管理要求	密码机的管理应提供图形化的专有软件进行管理，专有软件采用安全的方式与密码机连接，如采用信道加密的方法。密码机具备管理端口，管理端口与其他端口独立。管理端口是以太网口和串口。 采用串口管理模式应在通过安全控制检查后，采用人机接触的方式进行管理；采用以太网口管理模式应具有验证合法主机 IP 地址的功能，仅当口令认证通过后，方可进行管理工作。 密码机工作状态至少有两种：1）指令权限开放状态，该状态下，所有指令均可以使用，可以进行密钥的生成、注入、更新、导出等操作；2）指令权限受限的状态，该状态下，部分指令无法使用，无法进行密钥的生成、注入、更新、导出等操作。密码机指令权限开放状态和指令权限受限状态的转换应通过专有软件进行，转换过程中，应在授权安全介质

技术指标		指标参数
		（IC 卡、Key 等）接入的情况下进行。
	设备管理	在有远程集中管理需求时，密码机可具有设备远程集中管理功能，远程集中管理应提供专用的图形化设备管理客户端软件
	安全性要求	密码机应具备国家密码管理局颁布的商用密码产品型号证书。 配置安全自主可控型号。
	安全服务要求	密码机通过密码服务命令报文对用户提供安全服务，实现安全功能。 密码机的底层软件应采用模块化设计，防止不同功能模块相互影响。密码机应通过技术措施防止用户的非法调用。 密码机的主机服务支持 TCP/IP 通讯模式。应用系统向密码机请求密码服务时，按指令格式组合成正确的命令报文，发送给密码机，并等待接收密码机的应答报文。

7.1.3.5.10 持续威胁检测与溯源系统（APT）

指标项	具体要求
兼容性	1、产品及其依赖项满足《GB/T 36572-2018 电力监控系统网络安全防护导则》相关要求，应实现自身的安全，应安全、可控、可靠。 2、产品及其依赖项满足《GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求》3 级。
本体安全	1、产品及其依赖项满足《GB/T 36572-2018 电力监控系统网络安全防护导则》相关要求，应实现自身的安全，应安全、可控、可靠。 2、产品及其依赖项满足《GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求》3 级。 3、可限制仅特定地址登录； 4、远程管理设备时，应建立安全的通信协议；
硬件要求	硬件参数：规格：2U，CPU：≧64，内存：≧256 GB ，硬盘容量：≧48T，冗余电源，接口：2 千兆电口+6 万兆光口（接口允许通过扩展槽或配置探针设备满足要求），以上光模块满配，支持 ipv4 和 ipv6 双协议栈。 若单台设备性能不满足，允许配置探针设备达到性能要求。
性能要求	总体性能要求： 事件处理性能≧10000 eps（事件数每秒） 网络层吞吐≥30Gbps，应用层吞吐≥10Gbps 若单台设备性能不满足，允许配置探针设备达到总体性能要求
功能要求	实现以下功能的产品及其依赖项，均为本产品的供货范围。 1、支持高级威胁检测； 2、支持日志检索； 3、支持恶意代码检测； 4、支持从流量中发现威胁，如：协议异常、网络欺骗；

指标项	具体要求
	5、支持通过设备对流量进行抓包分析，可定义抓包流量双向或单向、数量、IP 地址、端口或协议类型； 6、支持告警的深度行为分析，行为包括 DNS 解析行为、TCP/UDP 交互行为、WEB 访问行为、传输文件行为； 7、支持暴力破解行为检测，检测内容包含：攻击者 ip、受害者 ip、使用协议、爆破次数、爆破成功与否等； 8、支持异常访问行为检测，检测内容包括：源 ip、违规访问者类型、主机名、访问类型； 9、支持识别爬虫行为并给出分析结果； 10、支持策略定义，可根据工作流进行处置动作定义，且能根据威胁等级、攻击结果、事件类别进行联动策略定义； 11、具备网络行为分析能力，实现对网络攻击特别是新型网络攻击行为的分析和告警；

7.1.3.5.11 安全 U 盘

指标项	具体要求
兼容性	1、产品及其依赖项满足《GB/T 36572-2018 电力监控系统网络安全防护导则》相关要求，应实现自身的安全，应安全、可控、可靠。 2、产品及其依赖项满足《GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求》3 级。
本体安全	1、产品及其依赖项满足《GB/T 36572-2018 电力监控系统网络安全防护导则》相关要求，应实现自身的安全，应安全、可控、可靠。 2、产品及其依赖项满足《GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求》3 级。
硬件要求	1、单个安全盘设备容量>=32G 2、产品接口 USB3.0
功能要求	实现以下功能的产品及其依赖项，均为本产品的供货范围。 1、整盘数据加密。 2、文件数据存储加密，采用国密 SM4 算法。 3、文件数据传输加密，防止通过 USB 监听手段窃取数据。 4、采用专用文件系统和文件浏览器进行文件管理；病毒、木马无法访问和感染设备存储区及文件系统。 5、支持用户设备身份注册绑定。 6、支持禁用、读取、写入、删除、修改等权限控制；支持内外网权限区分管理。 7、身份认证后才能登录安全存储设备。 8、口令错误超限后设备自动锁定。 9、支持口令长度和复杂性管理。 10、支持管理员对入网的移动存储介质进行注册，可以对已注册的移动介质进行管理，包括授权、启用、停用、删除、取消注册、导出注册列表等。 11、支持客户端自主申请移动存储介质注册，管理员统一对申请进行审批。

指标项	具体要求
	12、支持 U 盘与终端进行点对点的授权，可以灵活控制单个 U 盘在不同终端上拥有不同的使用权限。
性能要求	1、写入速度>=100MB/s。 2、读取速度通>=100MB/s。

7.1.3.5.12 杀毒 U 盘

指标项	具体要求
兼容性	1、产品及其依赖项满足《GB/T 36572-2018 电力监控系统网络安全防护导则》相关要求，应实现自身的安全，应安全、可控、可靠。 2、产品及其依赖项满足《GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求》3 级。
本体安全	1、产品及其依赖项满足《GB/T 36572-2018 电力监控系统网络安全防护导则》相关要求，应实现自身的安全，应安全、可控、可靠。 2、产品及其依赖项满足《GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求》3 级。
硬件要求	1、存储容量>=32GB。 2、接口类型 USB2.0 或 USB3.0。
功能要求	实现以下功能的产品及其依赖项，均为本产品的供货范围。 1、支持杀毒软件离线升级。 2、不会因为操作失误如删除、格式化，而把杀毒 U 盘变成普通的 U 盘。 3、可对载入的文件自动扫描，实现实时保护，避免病毒传播。

7.1.3.5.13 国密服务器密码机

指标项	具体要求
兼容性	1、产品及其依赖项满足《GB/T 36572-2018 电力监控系统网络安全防护导则》相关要求，应实现自身的安全，应安全、可控、可靠。 2、产品及其依赖项满足《GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求》3 级。
本体安全	1、产品及其依赖项满足《GB/T 36572-2018 电力监控系统网络安全防护导则》相关要求，应实现自身的安全，应安全、可控、可靠。 2、产品及其依赖项满足《GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求》3 级。 3、可限制仅特定地址登录； 4、远程管理设备时，应建立安全的通信协议；
硬件要求	1、CPU 核数≥8，内存≥16GB，存储≥480G； 2、至少提供 4 个网络端口，2 个千兆电口，2 个万兆光口（满配光模块），支持 ipv4 和 ipv6 双协议栈； 3、冗余双电源； 4、工作电压：220V（32V～343V）；

指标项	具体要求
	5、采用国家密码管理局批准的硬件芯片实现各类密码算法，保证算法的高安全性； 6、采用双路物理噪声源芯片产生高质量的真随机数作为密钥，保证密钥的安全产生； 7、配置备份恢复介质数量≥10； 8、配置国密 USB Key 数量≥10，USB Key 需要满足本次招标的智能密码钥匙技术参数；
功能要求	实现以下功能的产品及其依赖项，均为本产品的供货范围。 1、支持管理和应用的安全控制。 2、支持远程管理功能。 3、支持运行监控与日志审计。 4、安全关机功能。 5、支持国产 SM1/SM2/SM3/SM4 等算法。 6、支持对密钥的全生命周期管理功能，包括密钥生成、安全存储、备份恢复等功能。 7、采用国家密码管理主管部门批准的双物理噪声源芯片，提供多路随机源。 8、设备软件需符合 《GB/T 36322-2018 信息安全技术 密码设备应用接口规范》和《GMT 0018-2012 密码设备应用接口规范》要求。 9、具备授权控制机制、密码机操作身份认证应符合《GB/T 15843 采用数字签名技术》的认证要求。 10、重要的密钥操作采用多人分离管理机制。
性能要求	1、SM1 加解密：≥300Mbps； 2、SM2 签名：≥30000 次/秒； 3、SM2 验签：≥20000 次/秒； 4、SM3 摘要生成：≥500Mbps； 5、SM4 加解密：≥500Mbps。
资质要求	提供产品需具备由国家密码管理局商用密码检测中心颁发的商用密码产品认证证书，且证书中产品标准和技术要求的安全级别为符合《GM/T0028 密码模块安全技术要求》安全模块二级要求。

7.1.3.6 配套设备参数要求

本项目涉及的配套设备，中标方均应随主设备配置完整、满配的光模块，具体数量及技术选型以贵州电网公司实际需求为准。

7.1.3.6.1 卫星时钟

设备类型	规格
卫星时钟	支持双时钟源，包括双北斗授时。 时钟应能通过网络接口直接向局域网发布标准时间，各工作站运行相应对时进程，保持全网时钟同步。

设备类型	规格
	时钟的误差应小于 1.0×10-6 秒。在时钟系统的操作面板上应显示年、月、日、星期、小时、分、秒。 具备不少于 2 光 2 电的网络接口，满配的光模块。电口支持千兆自适应及以上能力，光口支持万兆自适应及以上能力。 具备 IRIG-B 输入及输出光接口。 冗余双电源。 配天线（长度应可根据工程实际需求定制，长度 100-200 米） 系统通过竣工验收后，由原厂家提供 5 年免费上门维修服务。

7.1.3.6.2 瘦终端

指标项	技术要求
处理器	采用安全自主可控主处理芯片，CPU 四核 1.7GHz 或以上性能
内存	DDR4 ≥2GB
闪存容量	≥64GB eMMC
本机系统	可支持 UOS、麒麟、凝思、龙蜥、欧拉等云桌面客户端系统部署。
适配云桌面操作系统	可支持适配连接 UOS、麒麟、凝思、龙蜥、欧拉等云桌面服务端系统。
输出分辨率	支持 2560*1440
生物识别	支持电容式指纹识别
蓝牙	蓝牙 5.0
视频播放	格式：RM/RMVB，MKV，TS，FLV，AVI，VOB，MOV，WMV，MP4 编码：H.264，VC-1，WMV-HD，MPEG1/2/4 最
音频播放	格式：MP3，WMA，APE，Flac 比特率：MP3 64kbps ～ 320kbps，WMA 64kbps ～ 320kbps，APE/Flac≤1500Kbps
图片格式	JPG，BMP，GIF
I/O 接口	≥1*Type-C2.0 接口
I/O 扩展	配套 Type-C 拓展坞，应具有 PD 快充、千兆网口、≥3 口 USB 3.0、HDMI、VGA 等接口。
电源输入	交流 100-240VAC/50-60Hz，
电源输出	5V-3A
电源类型	外接型电源适配器
安装方式	立式、背挂、平铺式
其它	整机无旋转部件

7.1.3.6.3 运维终端

指标项	技术要求
处理器	8 核 2.3GHz 及以上，采用安全自主可控主处理芯片
内存	≥32GB

指标项	技术要求
磁盘容量	固态硬盘 512G，机械硬盘 1TB
本机系统	含国产安全操作系统
输出分辨率	最高支持 2560*1440
生物识别	支持电容式指纹识别
蓝牙	蓝牙 4.2
I/O 接口	≥1*Type-C2.0 接口，≥2*USB3.2 Gen1，1 个 HDMI，1 个千兆网口
I/O 扩展	可通过扩展坞外接多个 USB 接口
电源输入	交流 100-240VAC/50-60Hz
电源类型	外接型电源适配器
政府采购需求标准	应满足附件 3《政府采购需求标准》中对应投标产品形态的技术参数要求。

7.1.4 安全Ⅱ区、安全接入区

7.1.4.1 服务器技术要求

服务器主频均要求≥2.2GHZ，内存要求≥512GB。每台服务器配置≥2 路热插拔电源，每单路热插拔电源可满足设备满载运行要求，任意一路电源故障设备功能应不受影响。

服务器类型	配置
非 III 区服务器-容量型	1、2U 机架式服务器； 2、CPU: 配置≥2 颗安全自主可控 CPU；单颗 CPU 要求：X86 架构核数≥24，ARM 架构核数≥48 核 3、内存：内存容量≥256GB，类型 DDR4 及以上，频率≥2933MHZ； 4、系统盘：配置≥960GB SSD【2*480GB SSD】硬盘； 5、数据盘：配置≥48TB HDD 物理容量（如：12 块 4TB 硬盘）； 6、RAID：配置 RAID 阵列卡，支持 RAID0/1/5/10 等主流 RAID 技术； 7、网络：配置≥2*双光纤端口 10GE 以太网卡（含光模块）； 8、电源：配置≥2 路热插拔电源，每单路热插拔电源可满足设备满载运行要求，任意一路电源故障设备功能应不受影响。
非 III 区服务器-通用型	1、2U 机架式服务器； 2、CPU: 配置≥2 颗安全自主可控 CPU；单颗 CPU 要求：X86 架构核数≥24，ARM 架构核数≥48 核 3、内存：内存容量≥256GB，类型 DDR4 及以上，频率≥2933MHZ； 4、系统盘：配置≥960GB SSD【2*480GB SSD】硬盘； 5、数据盘：≥8TB HDD 物理容量； 6、RAID：配置 RAID 阵列卡，支持 RAID0/1/5/10 等主流 RAID 技术； 7、网络：配置≥2*双光纤端口 10GE 以太网卡（含光模块）； 8、电源：配置≥2 路热插拔电源，每单路热插拔电源可满足设备满载运行要求，任意一路电源故障设备功能应不受影响。

7.1.4.2 网络设备技术要求

本项目涉及的网络设备，中标方均应随主设备配置完整、满配的光模块，具体数量及技术选型以贵州电网公司实际需求为准。

7.1.4.2.1 万兆接入交换机

技术指标	要求
外观	机架式 1U 盒式交换机，前后通风
硬件架构	冗余电源；冗余风扇 满足安全自主可控要求，设备芯片采用安全自主可控
端口	≥48 口 SFP+万兆，≥6 口 QSFP40G/100GE
性能要求	1.交换容量≥4.8Tbps，包转发率≥2000Mpps 2.支持≥4 台堆叠（IRF）/VSS，或者跨设备 LACP 聚合、LACP 边缘端口支持三层转发 3.所有端口支持巨帧转发（≥9216bytes） 4.10G、40G 端口支持路由口、路由子接口功能 5.端口支持 LLDP 功能 6.支持 IPv4/V6 双栈
二层功能	1.VLAN≥4K，支持 STP/RSTP/MSTP 2.支持 DHCPrelay，且 server 地址不小于 2 个 3.支持基于端口的广播风暴/组播/未知单播抑制 4. 支持 M-LAG 或 vPC 或 DRNI 等跨机箱链路捆绑技术
三层功能	1.支持 IPv4/v6 双栈支持静态路由、OSPFv2/v3、ISIS/v6、BGP/4+等动态路由协议 2.支持 ECMP 3.支持 IPv4/v6 三层组播：PIM-DM/SM，IGMP/MLD 4.支持 VRRP
VXLAN 特性	1.支持 Vxlan 协议，且支持 BGP EVPN 协议 2.支持 VXLAN over IPv6 3.支持 IPv6 VXLAN over IPv4 4.支持 VxLAN OAM：VxLAN ping， VxLAN tracert
网络管理	1.支持 POAP/Ansible/ZTP 等设备零配置自动化部署功能 2.支持 NETCONF 标准接口 3.支持 SNMP 通过域名方式访问 4.支持 NTP 客户端，支持时区修正，支持基于 IP 和域名访问 sever 5.支持 Console、Telnet 和 SSH2 命令行配置等网管方式 6.支持单物理端口和聚合组本地镜像、远程镜像 7.支持流量统计功能 8. 支持 ERSPAN
无损特性	支持 RDMA 和 RoCE（RoCE v1 和 RoCE v2）

技术指标	要求
	支持 RoCE 流量可视：支持对 RoCE 流量 KPI 进行分析
安全服务	1.支持基本 ACL、扩展 ACL、基于时间 ACL 等安全防护技术 2.支持 AAA 认证，并支持用户分级管理和口令保护 3.支持设置 SNMPv3 加密 4.支持远程日志记录，指定记录服务器 IP 地址
配置	设备包含满配对应光模块；

7.1.4.2.2 千兆管理交换机

技术指标	要求
外观	机架式 1U 盒式交换机，前后通风
硬件架构	冗余电源；冗余风扇 满足安全自主可控要求，设备芯片采用安全自主可控
端口	≥48 口千兆电+≥4 个 SFP+万兆光，含满配对应光模块
性能要求	1.交换容量≥600Gbps，包转发率≥200Mpps 2.支持堆叠（IRF）/VSS，或者跨设备 LACP 聚合、LACP 边缘端口支持三层转发 3.所有端口支持巨帧转发（≥9216bytes） 4.10G、40G 端口支持路由口、路由子接口功能 5.端口支持 LLDP 功能 6.支持 IPv4/V6 双栈
二层功能	1.VLAN≥4K，支持 STP/RSTP/MSTP 2.支持 DHCPrelay，且 server 地址不小于 2 个 3.支持基于端口的广播风暴/组播/未知单播抑制
三层功能	1.支持 IPv4/v6 双栈支持静态路由、OSPFv2/v3、ISIS/v6、BGP/4+等动态路由协议 2.支持 ECMP 3.支持 IPv4/v6 三层组播：PIM-DM/SM，IGMP/MLD 4.支持 VRRP
网络管理	1.支持 POAP/Ansible/ZTP 等设备零配置自动化部署功能 2.支持 NETCONF 标准接口 3.支持 SNMP 通过域名方式访问 4.支持 NTP 客户端，支持时区修正，支持基于 IP 和域名访问 sever 5.支持 Console、Telnet 和 SSH2 命令行配置等网管方式 6.支持单物理端口和聚合组本地镜像、远程镜像 7.支持流量统计功能
安全服务	1.支持基本 ACL、扩展 ACL、基于时间 ACL 等安全防护技术 2.支持 AAA 认证，并支持用户分级管理和口令保护 3.支持设置 SNMPv3 加密 4.支持远程日志记录，指定记录服务器 IP 地址

7.1.4.2.3 负载均衡器

技术指标	要求
硬件架构	CPU 总核数≥4 核；配置内存≥32GB；磁盘存储空间≥500GB；采用安全自主可控 CPU，操作系统；
端口	总端口数≥10 个，其中千兆电口≥6 个、SFP 万兆光口≥4 个；
性能要求	1.4 层吞吐量≥30Gbps，7 层吞吐量≥20Gbps；(提供国家权威机构测试报告)； 2.四层最大并发连接数≥3000 万，七层最大并发连接数≥750 万，四层新建连接数 CPS≥100 万，七层新建连接数 RPS≥150 万； 3.Outbound 双向多链路负载均衡、基于全功能智能的 DNS 解析及 IP anycast 技术的多数据中心负载均衡功能； 4.单台整机管理界面提供基于某种编程语言自定义的流量控制方法； 5.支持 GeoLocation 全球 IP 地址数据库； 6.支持与服务器虚拟化环境深度结合。

7.1.4.2.4 万兆采集交换机

技术指标	要求
外观	机架式 1U 盒式交换机，前后通风
硬件架构	冗余电源；冗余风扇 满足安全自主可控要求，设备芯片采用安全自主可控
端口	≥48 口 SFP+万兆，≥6 口 QSFP40G/100G，满配的光模块
性能要求	1.交换容量≥4.8Tbps，包转发率≥2000Mpps 2.支持≥4 台堆叠（IRF）/VSS，或者跨设备 LACP 聚合、LACP 边缘端口支持三层转发 3.所有端口支持巨帧转发（≥9216bytes） 4.10G、40G 端口支持路由口、路由子接口功能 5.端口支持 LLDP 功能 6.支持 IPv4/V6 双栈
二层功能	1.VLAN≥4K，支持 STP/RSTP/MSTP 2.支持 DHCPrelay，且 server 地址不小于 2 个 3.支持基于端口的广播风暴/组播/未知单播抑制 4. 支持 M-LAG 或 vPC 或 DRNI 等跨机箱链路捆绑技术
三层功能	1.支持 IPv4/v6 双栈支持静态路由、OSPFv2/v3、ISIS/v6、BGP/4+等动态路由协议 2.支持 ECMP 3.支持 IPv4/v6 三层组播：PIM-DM/SM，IGMP/MLD 4.支持 VRRP
VXLAN 特性	1.支持 Vxlan 协议，且支持 BGP EVPN 协议 2.支持 VXLAN over IPv6 3.支持 IPv6 VXLAN over IPv4

	4.支持 VxLAN OAM：VxLAN ping， VxLAN tracert
网络管理	1.支持 POAP/Ansible/ZTP 等设备零配置自动化部署功能 2.支持 NETCONF 标准接口 3.支持 SNMP 通过域名方式访问 4.支持 NTP 客户端，支持时区修正，支持基于 IP 和域名访问 sever 5.支持 Console、Telnet 和 SSH2 命令行配置等网管方式 6.支持单物理端口和聚合组本地镜像、远程镜像 7.支持流量统计功能 8. 支持 ERSPAN
无损特性	支持 RDMA 和 RoCE（RoCE v1 和 RoCE v2） 支持 RoCE 流量可视：支持对 RoCE 流量 KPI 进行分析
安全服务	1.支持基本 ACL、扩展 ACL、基于时间 ACL 等安全防护技术 2.支持 AAA 认证，并支持用户分级管理和口令保护 3.支持设置 SNMPv3 加密 4.支持远程日志记录，指定记录服务器 IP 地址
配置	设备包含满配对应光模块；

7.1.4.3 安全设备技术要求

本项目涉及的安全及配套设备，中标方均应随主设备配置完整、满配的光模块，具体数量及技术选型以贵州电网公司实际需求为准。

7.1.4.3.1 边界防火墙

类别	功能与技术描述
硬件平台	≤2U 机架式，实际配置可插拔冗余电源；满足国产品牌要求，要求采用安全自主可控芯片、操作系统，具备完整自主知识产权；必须独立专业防火墙设备，非插卡式扩展的防火墙设备。
硬件规格	CPU 核数≥4，存储容量≥1T SSD，内存≥64G；实际配置千兆电接口≥8，千兆光接口≥4，万兆光接口≥8（端口可通过扩展槽位扩展满足），扩展槽数量≥2；支持额外扩展 Bypass 插卡（可设备自带接口支持），满配对应光模块
性能要求	网络层吞吐量≥100Gbps，应用层吞吐量≥40Gbps，防火墙吞吐量≥40Gbps；IPS 吞吐量≥20Gbps；防病毒吞吐量≥18Gbps；最大并发连接数≥3000 万；每秒新建连接数≥80 万；IPSEC 吞吐量≥2.8Gbps；SSL VPN 用户数≥4000
访问控制	支持基于 IPV4/IPV6 的接口/安全域、地址、用户、服务、应用和时间的防火墙访问控制策略
	支持基于 IPV4/IPV6 的接口/安全域、地址、用户、服务、应用和时间的会话控制策略，包括总连接数控制、每秒总新建连接数控制、每 IP 总连接数控制、每 IP 新建连接数控制。
入侵防御	支持并开通 网络入侵检测及防御功能，入侵防御事件库事件数量不少于 12000 条

类别	功能与技术描述
	可基于 IP 地址、网段、用户、时间、VLAN、协议类型等条件设定入侵防御模块的检测事件及响应方式。
	提供 SQL 注入攻击、XSS 攻击的检测和防御功能，对 Web 服务系统提供保护；
防病毒	支持并开通对 HTTP、FTP、SMTP、POP3、IMAP 协议的病毒检测和过滤功能；
	基于主流杀毒引擎，支持对文件感染型病毒、蠕虫病毒、脚本病毒、宏病毒、木马、恶意软件等过滤
	支持 10 层以上压缩文件
	防病毒功能开启后，整机处理性能衰减不超过 30%
威胁情报	支持本地离线库在线更新，离线更新。
	支持失陷检测情报分类：勒索软件、挖矿软件、网银木马、窃密木马、黑客工具、后门软件、僵尸网络、常规木马、矿池数据、APT 攻击及其他远控等风险流量进行识别和过滤。可对不同类别风险 IP 流量进行记录日志或者阻断一定时间。
安全检测	支持 DoH 加密域名解析服务，对解析流量加密处理。
	支持联动云端威胁情报中心，可通过云端安全检查系统进行攻击识别，识别的攻击类型应至少包含：后门、远控木马、DDOS、挖矿、银行木马、APT、DGA、黑客工具、勒索软件、数据窃取、蠕虫、钓鱼网站、黄赌毒等威胁。
WAF 能力	支持 WEB 防护功能，支持对 100 个站点制订 Web 应用防护策略；
	支持自定义 WEB 安全防护事件，可对 HTTP 请求回应的头、体检查；
	支持自定义 WEB 安全防护事件，可以对请求参数、各个头域、内容关键字、文件类型等进行灵活组合生成策略
弱口令	支持弱口令密码检查
行为管理及流量控制	支持并开通基于 DPI 和 DFI 技术的应用特征识别及行为控制，应用识别的种类不少于 5000 种；支持并开通基于 URL 分类库的 WEB 访问管理，URL 分类库规模不少于 2000 万条
VPN	支持并开通 IPSec VPN、GRE VPN，并且支持从管控平台查询到每条 ipsec 隧道、gre 隧道的实时包、抖动、延迟数据以图形化界面进行展示
	支持并开通 SSL VPN，支持证书认证。
	支持多台防火墙设备在管控平台进行 2 种及以上的 vpn 隧道的配置和管理，并实时上报 vpn 隧道状态在控制平台以图形化界面进行展示。
国密	支持加密卡或软件方式，支持 SM2，SM3，SM4 国密算法。
网络特性	支持 VXLAN 功能，支持跨局域网络建立二层转发。
	支持标准 DNS 服务器功能，支持多种 DNS 记录 ，包括不限于 A ，AAA，PTR 记录。
	支持 DNS 透明代理功能，可将指定范围内的 DNS 请求自动重定向至管理员指定的 DNS 服务器，且支持多台 DNS 服务器的负载均衡。
系统管理	支持设备 web 页面抓包功能，支持基于接口，协议、地址类型（ipv4/ipv6）、客户端到防火墙、防火墙到目的服务器以及全部流量的匹配方式进行抓包；支持基于接口的入流量、出流量、双向流量的接口镜像功能
	支持基于并发会话数量的 TOP100 用户的展示数据和 TOP10 应用的并发数量曲线图，并发数量曲线图的统计周期包括小时、天、7 天和 30 天。

类别	功能与技术描述
	WEB 界面的网络调试功能，支持 PING、TRACEROUTE、TCP 探测方式，支持模拟数据流穿过设备时各个功能模块处理流程以及结果进行展示。

7.1.4.3.2 堡垒机

指标项	具体要求
兼容性	1、产品及其依赖项满足《GB/T 36572-2018 电力监控系统网络安全防护导则》相关要求，应实现自身的安全，应安全、可控、可靠。 2、产品及其依赖项满足《GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求》3 级。
本体安全	1、产品及其依赖项满足《GB/T 36572-2018 电力监控系统网络安全防护导则》相关要求，应实现自身的安全，应安全、可控、可靠。 2、产品及其依赖项满足《GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求》3 级。 3、远程管理设备时，应建立安全的通信协议。
授权要求	支持≧1500 个资产。
硬件规格	1、CPU 核数≥8，内存≥32GB，存储≥4T。 2、网络接口，配置≧（2 千兆电口+2 万兆光口），以上光模块满配。支持 ipv4 和 ipv6 双协议栈。 3、设备尺寸≤2U 标准机箱。
安全及管理	1.配置国密密码卡，实现通信数据的机密性和完整性；实现访问控制信息和日志记录的完整性保护；计量自动化系统为等保三级系统，国密密码卡应符合《GM/T0028 密码模块安全技术要求》安全二级及以上要求； 2.配置国密 USB Key 数量≥30，USB Key 需要满足本次招标的智能密码钥匙技术参数。 3.配置 CA 机构个人数字证书 10 套≥5 年授权。 4.支持审计日志自动、手动备份。日志最少保留 6 个月。 5.支持标准 SNMP 管理协议，支持 syslog 等标准日志格式外发。 6.实时监控系统 CPU、内存、磁盘的使用情况，支持 CPU、内存、磁盘使用超过阈值告警。
部署能力	1、支持 IPv6、IPv4 双协议栈。 2、物理旁路单臂部署，以逻辑网关方式工作；不改变现有网络结构。 3、单机部署、双机热备（HA）部署、分布式部署。 4、支持 B/S 运维。 5、支持 SNMP 协议：可对外提供终端设备的 CPU 利用率，内存利用率，磁盘空间利用率、网络等信息，支持 SNMP trap 告警外发；支持 Syslog 协议外发日志。
支持协议	1、字符协议：SSHv1、SSHv2、TELNET。 2、图形协议：RDP、VNC。 3、文件传输协议：FTP、SFTP、RDP 磁盘映射、RDP 剪切板。

指标项	具体要求
	4、协议代理审计模块：部署于 Liunx 服务器上，用于发布非标准协议或应用客户端并进行审计。
分权分域	1、系统内置系统管理员、审计管理员、安全管理员。 2、系统管理员可针对不同用户指定不同的管理权限，可设定用户（组）和资源（组）的管理范围。
用户管理	1、用户登录认证方式支持静态口令认证、手机动态口令认证、USB Key（数字证书）认证、AD 域认证、Radius 认证等认证方式；并支持各种认证方式和静态口令组合认证。 2、支持批量导入、导出用户信息。 3、支持用户手动添加、删除、编辑、设定角色、单独指定登录认证方式、设定用户有效期。 4、支持对用户指定限制登录 IP、登录时间段等规则。 5、支持口令有效期设置，用户账号口令到期强制用户修改自身口令。 6、支持登录控制台会话超时时间设置，用户在指定时间内无操作自动注销当前会话。 7、支持设定访问锁定策略，达到限制主账号密码输入错误次数和锁定时间的目的。
资源管理	1、支持服务器资源、网络设备资源、数据库资源、安全设备资源、C/S 资源、B/S 资源。 2、支持“内置应用发布服务器功能”，如无此功能，针对 C/S 架构的资产管理，需要单独配置外置应用发布服务器。 3、支持批量导入导出资源；支持手动添加、删除、编辑、查询资源。 4、支持资源的单点登录。
运维授权	1、支持一对一、一对多、多对多授权，如将单个资产授权多个用户，一个用户授予多个资产，用户组向资产组授权。 2、支持按授权名称、用户名称、用户账号、资源名称、资源地址、资源账号查询已授权信息。 3、支持在授权基础上设定双人复核登录，登录时必须经过第二人授权后才能登录。
账号托管	3、支持定期变更目标设备真实口令。 4、支持密码策略设置。
审计日志	1、支持监控正在运维的会话，信息包括运维用户、运维客户端地址、资源地址、协议、开始时间等并可以实时阻断（支持命令黑名单和命令审批规则）。 2、对字符命令方式的访问可以审计到所有交互内容，可以还原操作过程的命令输入和结果输出。 3、图形资源访问时，支持键盘、剪切板、窗口标题、文件传输记录，并且对图形资源的审计回放时。 4、自定义审计查询条件，包括：时间范围、用户与用户 IP、资源 IP、命令关键字条件。 5、提供用户统计报表和系统运行报表并支持导出。

7.1.4.3.3 费控密码机

技术指标		指标参数
硬件设备	物理端口	标准机架式设备，应可放入 19 英寸标准机架，应至少包含以下端口： 电源端口、密码服务以太网端口、管理以太网端口、管理串口、打印口、密钥销毁触发装置。
	随机数发生器	随机数产生器应采用国家密码管理局批准使用的多片多路物理噪声源芯片
	可靠性	平均无故障工作时间应不低于 30，000 小时
	并发访问	>=2048
功能、性能、安全等要求	初始化功能	密码机应具备初始化功能，实现设备的原始状态到工作状态的转换。初始化操作应至少包括设置设备主密钥、制作开机安全介质、制作授权安全介质、制作备份安全介质、设置设备参数、设置授权。 XX 密码机的初始化，除必须由厂商进行的操作外，系统配置、密钥管理、管理员管理等关键安全操作均应由用户方设备管理人员完成，密码机应提供图形化界面专用管理软件。
	密码运算	密码机应配用国家密码管理局认可的密码算法 SM1、SM2、SM3、SM4，采用硬件实现 SM1、SM2、SM3 和 SM4 算法。 SM1 算法加解密速率≥150Mbps SM2 算法签名速率≥6000 次/秒 SM2 算法验签速率≥4000 次/秒 SM3 算法运算速率≥700Mbps SM4 算法加解密速率≥700Mbps
	对称密码算法	密码机应配有 SM1 对称密码算法和 SM4 对称密码算法，SM1 密码算法的实现使用国家密码管理局指定的密码算法芯片，SM4 密码算法的实现遵循 GM/T0002-2012。 对称密码算法的工作模式应至少包括 ECB、CBC、CFB 和 OFB 四种模式。
	公钥密码算法	密码机应配用 SM2 非对称密码算法，SM2 密码算法的实现遵循 GM/T0003-2012。
	密码杂凑算法	密码机应配用 SM3 杂凑算法，SM3 杂凑算法的实现遵循 GM/T0004-2012。另外，SM2 密码算法用于数字签名验签和计算消息认证码时，算法要求配用 SM3 杂凑算法，在 SM2 密码算法中使用的 SM3 杂凑算法的实现遵循 GM/T0004-2012。
	密钥管理	密码机应具备完整的密钥管理机制，密钥保护涵盖密钥的产生、注入、导入/导出、备份/恢复、查询和销毁整个生命周期，密码机必须保证密钥在生存周期的各个环节的安全性。密钥安全风险是指业务系统中的各种主控密钥和应用密钥在分发、保存、使用中的泄露、篡改、非法替换的风险。密

技术指标		指标参数
		码机应提供密钥安全性的设计保障。安全性设计应有明确的密钥保护措施和方法来消除密钥安全风险。
	访问控制	密码机应提供访问控制功能，防止非授权访问密码机引起的安全风险。访问控制包 括密码机的管理、使用和业务等方面内容
	管理要求	密码机的管理应提供图形化的专有软件进行管理，专有软件采用安全的方式与密码机连接，如采用信道加密的方法。密码机具备管理端口，管理端口与其他端口独立。管理端口是以太网口和串口。 采用串口管理模式应在通过安全控制检查后，采用人机接触的方式进行管理；采用以太网口管理模式应具有验证合法主机 IP 地址的功能，仅当口令认证通过后，方可进行管理工作。 密码机工作状态至少有两种：1）指令权限开放状态，该状态下，所有指令均可以使用，可以进行密钥的生成、注入、更新、导出等操作；2）指令权限受限的状态，该状态下，部分指令无法使用，无法进行密钥的生成、注入、更新、导出等操作。密码机指令权限开放状态和指令权限受限状态的转换应通过专有软件进行，转换过程中，应在授权安全介质（IC 卡、Key 等）接入的情况下进行。
	设备管理	在有远程集中管理需求时，密码机可具有设备远程集中管理功能，远程集中管理应提供专用的图形化设备管理客户端软件
	安全性要求	密码机应具备国家密码管理局颁布的商用密码产品型号证书。 配置安全自主可控型号。
	安全服务要求	密码机通过密码服务命令报文对用户提供安全服务，实现安全功能。 密码机的底层软件应采用模块化设计，防止不同功能模块相互影响。密码机应通过技术措施防止用户的非法调用。 密码机的主机服务支持 TCP/IP 通讯模式。应用系统向密码机请求密码服务时，按指令格式组合成正确的命令报文，发送给密码机，并等待接收密码机的应答报文。

7.1.4.3.4 网络终端接入核查设备

指标项	具体要求
兼容性	1、产品及其依赖项满足《GB/T 36572-2018 电力监控系统网络安全防护导则》相关要求，应实现自身的安全，应安全、可控、可靠。 2、产品及其依赖项满足《GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求》3 级。

指标项	具体要求
本体安全	1、产品及其依赖项满足《GB/T 36572-2018 电力监控系统网络安全防护导则》相关要求，应实现自身的安全，应安全、可控、可靠。 2、产品及其依赖项满足《GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求》3 级。 3、可限制仅特定地址登录。 4、远程管理设备时，应建立安全的通信协议。
授权要求	支持≧1500 个终端数。
硬件要求	1、CPU 核数≧8；内存大小：≧32G，硬盘容量：≧960G。 2、配置冗余电源。 3、网络接口，配置≧（2 千兆电口+2 万兆光口），以上光模块满配。支持 ipv4 和 ipv6 双协议栈。 4、设备外形及安装：2U 及以下标准机架。
功能要求	实现以下功能的产品及其依赖项，均为本产品的供货范围： 1、支持扫描识别网络内的终端设备及类型并展示。 2、支持 802.1X：在网络接入层做准入认证、根据认证授权情况确定是否能访问网络。 3、支持 Portal：当新终端接入交换机时，交换机发现该终端未经身份认证，则将其浏览器请求重定向至 Portal 认证页面，用户通过身份认证成功后即可正常访问网络。 4、支持 MAB：启用此特性后，当通过 802.1X 认证的端口连接的设备是无法进行交互认证的设备时，交换机就会尝试使用基于 Mac 地址的免认证特性来识别客户端。 5、支持 SNMP 协议：可对外提供终端设备的 CPU 利用率，内存利用率，磁盘空间利用率、网络流量使用信息等信息，支持 SNMP trap 告警外发；支持 Syslog 协议外发日志。

7.1.4.3.5 万兆正向隔离装置

类别	功能与技术描述
总体需求	万兆物理隔离；
	机架式安装，含机架安装套件；
	具备电力专用安全防护设备的检测证明；
	具备公安部颁发的《计算机信息系统安全专用产品检测证书》；
	应通过有关部门组织的电磁兼容性检测；
	采用非 Intel 指令系统（及兼容）的 RISC 微处理器构筑内外网隔离系统；
	嵌入式安全操作系统，去除不需要的所有系统服务；
功能要求	本身应能够一定程度防御常见的网络攻击，包括 ARP Attack、Ping Attack、Ping of Death Attack、Smurf Attack、Unreachable Host Attack、Land Attack、Teardrop Attack、Syn Attack 等；
	数据单向传输，1bit 返回信息；
	表示层与应用层数据完全单向传输，即从安全区 III 到安全区 I/II 的 TCP 应答禁止携带应用数据；

类别	功能与技术描述
	透明工作方式：虚拟主机 IP 地址、隐藏 MAC 地址；
	基于 MAC、IP、传输协议、传输端口及通信方向的综合报文过滤与访问控制；
	支持 NAT；
	隔离设备的关键芯片和元器件都进行产品老化试验，所有的隔离设备在出厂前必须经过不少于 72 小时连续通电测试，并提供相关质量报告；
	防止穿透性 TCP、UDP 联接；
	配置冗余电源，支持双机热备；
	支持“单进单出”“双进单出”“双进双出”等多种连接方式；
	支持系统告警，支持完备的安全事件告警机制，当发生非法入侵、装置异常、通信中断或丢失应用数据时，可通过网络向第三方日志告警管理系统输出报警信息，日志格式遵循 Syslog 标准；
	维护管理方便、安全：基于证书的管理人员认证，图形化的管理界面；
性能要求	CPU 主频≥1.8GHz；
	CPU 核心≥12 核；
	万兆状态下数据传输率≥5Gbps；
	最大并发联接数≥10000；
	数据包转发延迟＜1ms（90%吞吐量）；
	满负荷数据包丢弃率为 0%（90%吞吐量）；
	内网网络接口：至少包含 4 个 GE 业务接口、4 个 SPF+接口，1 个 GE 管理接口，1 个 RS232、1 个 USB 口，网络速率自适应，满配的光模块；
	外网网络接口：至少包含 4 个 GE 业务接口、4 个 SPF+接口，1 个 GE 管理接口，1 个 RS232、1 个 USB 口，网络速率自适应，满配的光模块；
	平均无故障时间＞60000 小时（100％负荷）；
质保要求	含五年原厂保修和软件升级。

7.1.4.3.6 万兆反向隔离装置

类别	功能与技术描述
总体需求	万兆物理隔离；
	机架式安装，含机架安装套件；
	具备电力专用安全防护设备的检测证明
	具备公安部颁发的《计算机信息系统安全专用产品检测证书》；
	具备国家密码管理局商用密码检测中心颁发的《商用密码产品认证证书》
	应通过有关部门组织的电磁兼容性检测；
	采用非 Intel 指令系统（及兼容）的 RISC 微处理器构筑内外网隔离系统；
	配置本设备用加密卡，并配套提供对侧接口服务器用加密卡，以提升传输过程中的加密性能。
	嵌入式安全操作系统，去除不需要的所有系统服务；
功能要求	本身应能够一定程度防御常见的网络攻击，包括 ARP Attack、Ping Attack、Ping of Death Attack、Smurf Attack、Unreachable Host Attack、Land Attack、Teardrop Attack、Syn Attack 等；

类别	功能与技术描述
	具有基于数字证书的数据签名/解签名功能，具有电力加密算法进行数字加密功能；
	具有应用数据内容有效性检查功能；
	具有 E 文本编码检查功能；
	实现两个安全区之间的非网络方式的安全的数据传递；
	透明工作方式：虚拟主机 IP 地址、隐藏 MAC 地址；
	支持 NAT；
	基于 MAC、IP、传输协议、传输端口及通信方向的综合报文过滤与访问控制；
	防止穿透性 UDP 联接；
	数据单向传输，1bit 返回信息；
	配置冗余电源，支持多机阵列；
	支持“单进单出”“双进单出”“双进双出”等多种连接方式；
	支持系统告警，支持完备的安全事件告警机制，当发生非法入侵、装置异常、通信中断或丢失应用数据时，可通过网络向第三方日志告警管理系统输出报警信息，日志格式遵循 Syslog 标准；
	内网网络接口：至少包含 4 个 GE 业务接口、4 个 SPF+接口，1 个 GE 管理接口，1 个 RS232、1 个 USB 口，网络速率自适应，满配的光模块；
	外网网络接口：至少包含 4 个 GE 业务接口、4 个 SPF+接口，1 个 GE 管理接口，1 个 RS232、1 个 USB 口，网络速率自适应，满配的光模块；
	维护管理方便、安全：基于证书的管理人员认证，图形化的管理界面。
性能要求	CPU 主频≥1.8GHz；
	CPU 核心≥12 核；
	密文有效网络吞吐率≥4Gbps；
	数字签名速率≥30000 次/秒；
	最大并发连接数≥10000；
	数据包转发延迟＜1ms（90%吞吐量）；
	满负荷数据包丢弃率为 0%（90%吞吐量）；
	平均无故障时间＞60000 小时（100%负荷）；
质保要求	含五年原厂保修和软件升级。

7.1.4.3.7 运维区防火墙

类别	功能与技术描述
安全认证	满足国家安全产品有关认证要求。
产品架构	基于自主可控芯片的多核 CPU 架构
系统安全性	采用防火墙专用操作系统
	支撑系统不提供多余的网络服务
	系统不含任何高、中风险安全漏洞
冗余电源	提供双电源供电，并支持故障告警
设备支撑	配置设备机箱配套支架，设备高度不大于 2U

端口数量及类型	业务口要求：提供 2 个万兆光接口、8 个千兆光接口用于网络通讯，提供管理接口和 HA 端口。满配对应光模块
整机吞吐量	数据包吞吐量≥15Gbps
最大并发连接数	最大并发连接数≥300 万
每秒新建连接数	每秒新建连接数≥10 万
静态路由	最大静态路由条数≥1000 条
	支持基于源、目的 IP 地址的策略路由能力
访问控制策略	最大访问控制策略条数≥10000 条、最大地址集建立数目≥30000 条、最大服务集建立数目≥30000 条，最大域名对象数目≥3000 条
工作模式	1.支持透明模式
	2.支持路由模式
	3.支持混合模式
协议支持	1.支持 TCP、UDP 协议
	2.支持 IPv4、IPv6、ICMP、GRE（无需绑定物理接口）、VRRP、OSPF、BGP、RIP、SNMP 等协议
	3.支持 ARP、VLAN Trunk、QinQ 等协议
链路捆绑	1.支持多条链路的捆绑及链路间的负载均衡
NAT 功能	1.支持静态网络地址转换(Static NAT)
	2.支持动态网络地址转换(Dynamic NAT)
	3.支持网络地址及端口转换(PAT)
ALG 功能	1.能够识别常见应用协议并进行应用层处理
	2.支持对动态端口协议进行识别并控制
状态监测	1.支持基于会话的安全过滤，根据会话表放行或阻断数据包
	2.支持会话管理表，能够对特定的会话直接操作（删除等）
	3.支持会话超时保护，无报文的会话在一定时间后自动删除
流量及带宽管理	1.支持对 IP、IP 组、协议及端口进行带宽控制
	2.支持对最大与最小带宽进行限制
	3.支持根据 IP 地址限制并发 session 数量
连接控制	1、支持对源/目的地址对象、应用等设置并发和新建会话数量
	2、支持展示被拦截的 IP、地址对象、被拒次数、最近被拒时 间等信息
策略优化	1.支持分析失效、冗余、冲突的策略
	2.支持对策略有效性进行统计，支持策略的命中统计
	3.支持策略查询及导出功能
	4.支持批量修改策略配置信息，如批量禁用策略、批量删除 策略等
IPV6 功能	1.支持 IPv6 协议栈，支持 IPv6 地址的正确解析
	2.支持 IPV6 的 ACL 过滤
	3.支持 IPv6 的路由协议，包括 IPv6 的静态路由、动态路由（含 OSPFv3）和策略路由
	4.支持 IPV6 的状态检测功能
	5.支持 IPV6 的报文检测功能
	6.支持 NAT64、IPv4/IPv6 双栈
	7 支持 IPV6 DDOS 等攻击防护功能
	8.设备纯 IPv4 及纯 IPv6 的性能要求一致

攻击防御	1.支持对常见攻击方式进行检测与防御（DDOS、特殊报文、扫描攻击、特殊控制报文攻击等）
	2.抵抗各种典型的拒绝服务攻击，包括 SYN FLOOD，UDP FLOOD，ICMP FLOOD，IP 碎片包攻击，源 IP 地址欺骗攻击
	3.支持数据包的深度检测
	4.支持基于源及目的 IP 地址的并发连接数的控制
访问控制	1.支持基于域名的访问控制，且无需改变主机、终端的域名解 析配置
	2.支持基于 IP 地址的访问控制
	3.支持基于端口的访问控制
	4.支持基于协议的访问控制
	5.支持基于时间的访问控制
	6.支持基于连接的访问控制
	7.支持默认禁止策略
	8.支持用户自定义安全策略
黑白名	1.支持黑名单功能，被列入黑名单的 ip 及 ip 地址段，禁止所有访问，支持有效期设置，并提供黑名单增删 api 接口；黑名 单条码不少于 3000 条；
	2.支持白名单功能，被列入白名单的 ip 及 ip 地址段，放行所有访问，支持有效期设置，并提供白名单增删 api 接口；
IPSEC VPN	1.支持 IPSEC VPN。支持对隧道内流量进行监控
	2.支持多种（国际、国内）加密算法
应用控制	1．支持识别并控制各种常见应用
	2.支持自定义应用特征
入侵防御	1.支持告警和拦截非法、不正常、含攻击行为的报文
	2.支持手动自定义攻击规则库
	3.支持在线、离线、手动升级规则库
	4.至少支持威胁阻断模式、威胁监测模式
URL 过滤	1.支持黑白名单、恶意 URL 过滤
	2.内置恶意 URL 库，并支持在线、离线、手动更新
	3.支持自定义 URL 和阻断界面内容
	4．支持 URL 通配符，可通过通配符阻断某网站二级网站或页面
病毒过滤	1.支持对数据报文及文件进行病毒查杀
	2.支持对病毒报文及文件进行查杀、隔离等操作
	3.可拦截典型木马攻击行为
	4.支持在线、离线、手动更新规则库
管理方式	1.支持本地串口管理、远程管理、集中管理、分级管理等
	2.支持多主控台同时管理
	3.支持 HTTPS，SSH 等管理方式
	4.支持设置、查询和修改安全策略
	5.支持鉴别失败管理
	6.支持设备及策略集中管理
系统管理	1.支持自身状态监控，支持 snmp 管理，支持流量监测，提供支持设备状态监控、流量监控的北向 api 接口
	2.支持带外网管接口

	3.支持 Trap 协议
	4.支持配置备份、NTP 时间同步等
用户管理	1.支持对授权管理员的口令鉴别方式
	2.支持管理员权限划分
	3.支持对授权管理员、主机和用户进行身份鉴别
日志管理	1.支持流量日志、事件类日志、操作类日志、运行类日志及用户日志
	2.支持本地日志导出、日志清空、日志查询等
	3.支持 SYSlog 等方式发送至多个日志服务器，提供 syslog 范式化服务
	4.支持设置日志传输参数
行为审计	1.支持用户行为审计
	2.支持审计数据查询
自身安全性	1.支持配置限定用户登陆的 IP 地址范围
	2.支持 SSH、HTTPS 等加密方式进行远程访问
	3.支持对用户口令进行加密保存
	4.支持用户口令复杂度设置及检查
	5.支持最大登录失败重试次数设置
	6.支持用户登录超时时间设置
	7.支持双因子认证方式
	8.应保证所用的操作系统不存在安全漏洞
对外接口	1.设备应具备开放性、可扩展性，并提供开放接口，其中对外接口包括：允许策略增删改查、特征库版本、运行状态、策略命中情况等信息
	2.支持通过 SYSlog 方式以 UDP 发送日志对接监测系统，并可配合完成联动测试
可靠性与可用性	1.应提供 MTBF(Mean Time Between Failure)和 MTTR(Mean Time To Repair)指标，其中 MTBF 不小于 5 万小时，MTTR 不大于 2 小时
	2.支持电源冗余，电源冗余单元应支持热插拔功能
	3.支持软件防护加载、升级失败回滚
	4.支持 trouble-shooting 和性能监控、故障跟踪能力
	5.支持双机备份（双机热备、双机冷备）功能
	6.支持双机配置同步功能
	7.支持主备切换会话保持
	8.支持在关闭防火墙策略时，能够正常路由转发数据包
	9.支持设备状态监测、端口状态监测、链路连通性状态监测，可根据监测的设备状态，实现秒级的高可用切换，保障业务连续性
	10.应具有软件故障的监视功能，一旦软件出现死循环等重大故障时，应能自动再启动，并作出即时故障报告信息
供应链稳定性	具备供应链稳定性
售后服务	整机软硬件 5 年免费原厂维护、管理软件升级维护及技术支持服务（含特征库、规则库、许可等各种软件限制性的授权服务）

7.1.4.3.8 千兆纵向加密认证网关

指标项	技术参数
参数要求	通过国家有关机构认证； 具有公安部计算机信息安全产品质量监督检验中心出具的《检验报告》； 具备公安部颁发的《计算机信息系统安全专用产品检测证书》 具备国家密码管理局商用密码检测中心颁发的《商用密码产品认证证书》 采用专用服务器硬件和代码可控的安全操作系统，设备主处理芯片、操作系统满足安全自主可控要求； 本身应能够一定程度防御常见的网络攻击，包括 ARP Attack、Ping Attack、Ping of Death Attack、Smurf Attack、Unreachable Host Attack、Land Attack、Teardrop Attack、Syn Attack 等； 支持设备钥匙、工作参数的备份与恢复。 应通过有关部门组织的电磁兼容性检测； 应支持双机热备功能，在任一设备出现故障时能自动切换； 应具有可配置自动旁路功能，在紧急故障状态下，用户可以通过配置使能旁路所有安全策略或部分链路的安全策略的功能，使之作为透明桥接设备工作，必要时允许通过网线旁路。在旁路状态下，设备应有明显的警告提示。 采用国家密码管理局批准的电力专用密码算法对传输的数据进行保护，保证数据的真实性、机密性和完整性； 加密认证装置或加密认证网关之间支持基于电力数字证书的认证； 支持透明工作方式与网关工作方式，支持 NAT； 具有基于 IP、传输协议、应用端口号的综合报文过滤与访问控制功能； 加密认证网关支持对电力应用协议的特殊报文进行选择性加密保护； 符合《IP 加密认证装置技术规范》的技术要求，支持不同厂家设备的互通互联；支持由不同厂家纵向加密认证装置管理中心进行远程监控和管理。 装置必须能够识别、处理网络正常运行所需要的路由协议报文及其他协议报文； 装置必须能够识别、过滤、转发 802.1q 协议的报文，装置本地配置功能必须支持配置 VLanID。 网络接口：网络接口不少于 4 个 10/100/1000M，2 光口 2 电口，网络速率需要自适应，满配的光模块； 热备接口：具备双机热互备接口及相关软件； 外设接口：1 个 RS232 配置接口+1 个 IC 卡读卡器接口或 USBkey 接口； 最大并发加密隧道数：>=2000 条 1000M LAN 环境下，加密隧道建立延迟：<1s 明文数据包吞吐量：>=1900Mbps（200 条安全策略，1024 字节报文长度） 密文数据包吞吐量：>=600Mbps（200 条安全策略，1024 字节报文长度） 支持配置安全策略>=5000 条 数据包转发延迟：＜2ms （50%密文数据包吞吐量）

指标项	技术参数
	满负荷数据包丢弃率：0 设备电源：双电源； 质保要求：含五年原厂保修和软件升级。

7.1.4.3.9 入侵防御设备

指标项	具体要求
兼容性	1、产品及其依赖项满足《GB/T 36572-2018 电力监控系统网络安全防护导则》相关要求，应实现自身的安全，应安全、可控、可靠。 2、产品及其依赖项满足《GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求》3 级。
本体安全	1、产品及其依赖项满足《GB/T 36572-2018 电力监控系统网络安全防护导则》相关要求，应实现自身的安全，应安全、可控、可靠。 2、产品及其依赖项满足《GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求》3 级。 3、可限制仅特定地址登录。 4、远程管理设备时，应建立安全的通信协议。
硬件要求	硬件参数：规格：≤2U，CPU 核数：≧16，内存大小：≧32G，硬盘容量：≧1T，电源：冗余电源，接口：4 千兆电口+6 万兆光口，以上模块满配，支持 ipv4 和 ipv6 双协议栈。
功能要求	实现以下功能的产品及其依赖项，均为本产品的供货范围。 1、支持上传、下载、双向的文件内容过滤。 2、可准确地发现包括钓鱼攻击、恶意 SSL 证书、重定向攻击、获取权限、拒绝服务、漏洞利用等网络攻击行为。 3、提供统计分析面板，可将展示威胁统计、恶意 URL、恶意域名、恶意地址内容展示；并支持多时间维度筛选。 4、可在单条策略中启用病毒防护、入侵防御、网址过滤、文件过滤、文件内容过滤、终端过滤等安全功能选项。 5、支持安全策略的快速检索及基于名称、地址多维度的高级策略检索。 6、支持添加报表任务。生成可查看报表。 7、支持离线实现 IPS 特征库、威胁库更新。 8、访问控制规则支持模拟策略匹配，输入源目的 IP、端口、协议五元组信息，模拟策略匹配方式，给出最可能的匹配结果，方便排查故障，或环境部署前的调试。 9、支持针对 HTTP、FTP 协议内容检测与病毒查杀。 10、设备具备独立的入侵防护漏洞规则特征库。 11、设备具备独立的热门威胁库，防护类型包括木马远控、恶意脚本、勒索病毒、僵尸网络、挖矿病毒等。 12、支持本地威胁情报检测和威胁情报库离线升级。 13 安全策略支持基于源安全域、目的安全域、源用户、源地址/地区、目的地址/地区、VLAN 等多种方式进行访问控制。 14、支持 SNMP 协议：可对外提供终端设备的 CPU 利用率，内存利用率，

指标项	具体要求
	磁盘空间利用率、网络流量使用信息等信息，支持 SNMP trap 告警外发； 支持 Syslog 协议外发自身日志。
性能要求	整机吞吐量>=100G； IPS 吞吐>=20G； 最大并发连接数不小于 2000 万； 新建连接不小于 80 万/秒。

7.1.4.3.10 计量通信认证网关

指标项	具体要求
兼容性	本设备应兼容安全自主可控软硬件环境。 本设备应兼容电能计量安全费控密钥体系。
安全	1、产品及其依赖项满足《GB/T 36572-2018 电力监控系统网络安全防护导则》相关要求，应实现自身的安全、可控、可靠； 2、产品及其依赖项满足《GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求》3 级； 3、可限制仅特定地址登录； 4、远程管理设备时，应建立安全的通信协议。 5、采用专用服务器硬件和代码可控的安全操作系统；
硬件	1、网络接口：不少于 2 个千兆加密业务网口； 2、1 个管理网口，1 个串口 Console 口； 3、冗余交流电源。
功能	1、在主站与计量终端之间建立完全透明的、高强度加密传输链路 2、即插即用、无需配置 IP、路由等任何网络属性； 3、部署本设备对原网络系统“零”影响：无需更改原网络拓扑，无需修改上下游网络设备任何配置，无需应用系统做任何修改； 4、支持 SM2/SM3/SM4 等国家商用密码算法； 5、支持 RSA1024/2048/AES/SHA1/SHA2 等国际算法； 6、支持对称/非对称密钥管理体系，兼容计量数字证书系统； 7、支持任意网络设备或主机设备，支持任意主机操作系统与应用系统； 8、需提供计量终端接入认证服务模块，可以适配典型存量计量终端；
性能	1、网络加密延迟：＜35 微秒 2、加密带宽：900Mbps 3、加密算法：国密算法：SM2/SM3/SM4 以及国际算法 4、密钥/数据存储年限：＞15 年

7.1.4.3.11 数据库审计

指标项	具体要求
兼容性	1、产品及其依赖项满足《GB/T 36572-2018 电力监控系统网络安全防

指标项	具体要求
	护导则》相关要求，应实现自身的安全，应安全、可控、可靠。 2、产品及其依赖项满足《GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求》3 级。
本体安全	1、产品及其依赖项满足《GB/T 36572-2018 电力监控系统网络安全防护导则》相关要求，应实现自身的安全，应安全、可控、可靠。 2、产品及其依赖项满足《GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求》3 级。 3、可限制仅特定地址登录； 4、远程管理设备时，应建立安全的通信协议；
授权要求	数据库实例个数≥50;
硬件要求	硬件参数：规格：2U，CPU 核数：≧8，内存大小：≧16G，硬盘容量：≧4T，电源：冗余电源，接口：2 千兆电口+2 万兆光口，以上光模块满配，支持 ipv4 和 ipv6 双协议栈.
功能要求	实现以下功能的产品及其依赖项，均为本产品的供货范围。 1、支持对安全、自主、可控的数据库审计。 2、审计内容包括会话的终端信息、会话的主机信息、会话的操作信息等； 3、审计记录检索，支持通过访问来源信息（源 IP、业务主机端口、数据库名称、数据库用户、操作类型、表名、影响结果等、MAC 地址）方式进行检索； 4、查看日志详情，日志详情包括“时间、客户端 IP、目标数据库 IP、客户端 MAC、数据库类型、操作类型、客户端端口、响应时长、响应码、结果信息、客户端执行命令”等信息； 5、应用服务器对数据库的访问时，对数据库操作进行跟踪定位，包括数据库 SQL 执行情况、数据库返回值等。 6、会话回放，对用户从本次登录到退出这段时间内对数据库所做的所有操作按一定的时间间隔进行自动显示。 7、审计日志至少保留 180 天。 8、支持风险操作的实时监控及告警。风险信息包括“风险类型、风险次数、时间”等； 9、支持检测 SQL 注入及告警； 10、支持自定义风险规则。 11、支持 SNMP 协议：可对外提供终端设备的 CPU 利用率，内存利用率，磁盘空间利用率、网络流量使用信息等信息，支持 SNMP trap 告警外发；支持 Syslog 协议外发自身日志。
性能要求	1、SQL 审计处理能力≥10000/S。 2、吞吐流量≥2G/S。 3、检索亿级日志秒级响应

7.1.4.3.12 日志审计

指标项	具体要求

指标项	具体要求
兼容性	1、产品及其依赖项满足《GB/T 36572-2018 电力监控系统网络安全防护导则》相关要求，应实现自身的安全，应安全、可控、可靠。 2、产品及其依赖项满足《GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求》3 级。
本体安全	1、产品及其依赖项满足《GB/T 36572-2018 电力监控系统网络安全防护导则》相关要求，应实现自身的安全，应安全、可控、可靠。 2、产品及其依赖项满足《GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求》3 级。 3、可限制仅特定地址登录； 4、远程管理设备时，应建立安全的通信协议；
授权要求	支持≧1500 个 IP
硬件要求	硬件参数：规格：2U，CPU 核数：≧8，内存大小：≧16G，硬盘容量：≧8TB，电源：冗余电源，接口：2 千兆电口+2 万兆光口，以上光模块满配，支持 ipv4 和 ipv6 双协议栈
功能要求	实现以下功能的产品及其依赖项，均为本产品的供货范围。 资产管理： 1、能够将资产按照多种维度进行分组、组织结构、业务系统等，提供便捷的添加、修改、删除、查询功能； 2、支持自定义资产类型； 3、支持对资产标签内容进行查询和管理。 日志收集： 1、Syslog、SNMP Trap 等协议被动采集日志； 2、支持文件读取、日志代理等方式主动采集； 3、支持 API 等方式交互式采集日志； 集中管控： 1、支持日志范式化和归一化； 2、支持按周期的方式对原始日志与范式化后的日志进行本地存储和外置备份（根据《网络安全法》的相关规定，日志保存期限不少于 6 个月）； 审计管理： 1、支持对原始日志和范式化后的日志进行按条件检索； 2、支持对日志进行分析，生成告警信息，并发出通知。 3、可以对日志分析结果按条件进行检索。 日志转发： 1、支持 SNMP 协议：可对外提供终端设备的 CPU 利用率，内存利用率，磁盘空间利用率、网络流量使用信息等信息，支持 SNMP trap 告警外发；支持 Syslog 协议外发自身日志。 2、支持转发原始日志或归一化日志；
性能要求	1、日志处理总体性能≥2500EPS（事件数每秒）； 2、10 亿条日志量查询平均响应时间不超过 10 秒。

7.1.4.3.13 漏洞扫描

指标项	具体要求
兼容性	1、产品及其依赖项满足《GB/T 36572-2018 电力监控系统网络安全防护导则》相关要求，应实现自身的安全，应安全、可控、可靠。 2、产品及其依赖项满足《GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求》3 级。
本体安全	1、产品及其依赖项满足《GB/T 36572-2018 电力监控系统网络安全防护导则》相关要求，应实现自身的安全，应安全、可控、可靠。 2、产品及其依赖项满足《GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求》3 级。 3、可限制仅特定地址登录； 4、远程管理设备时，应建立安全的通信协议；
授权要求	支持≧1500 个 IP
硬件要求	硬件参数：规格：≤2U，CPU 核数：≧8，内存大小：≧32G，硬盘容量：≧4TB，电源：冗余电源，接口：2 千兆电口+2 万兆光口，以上光模块满配，支持 ipv4 和 ipv6 双协议栈
功能要求	实现以下功能的产品及其依赖项，均为本产品的供货范围。 1、支持动态发现 IT 环境中的资产； 2、支持手动录入资产； 3、支持主机资产的识别，同时获取资产存活状态、操作系统、端口、服务等信息。 4、兼容 CVE、CNNVD、CNVD 等主流漏洞库 ； 5、漏洞库支持离线升级。 6、支持常用及安全自主可控的系统漏洞、Web 漏洞、中间件漏洞、数据库漏洞、弱口令等发现能力； 7、支持扫描任务管理； 8、支持按需创建扫描任务，包括执行方式（包含立即执行、定时执行、周期执行）。 9、支持 SNMP 协议：可对外提供设备的 CPU 利用率，内存利用率，磁盘空间利用率等信息，支持 SNMP trap 告警外发；支持 Syslog 协议外发日志；
性能要求	1、支持主机漏扫并发 IP 数≧90。

7.1.4.3.14 持续威胁检测与溯源系统（APT）

指标项	具体要求
兼容性	1、产品及其依赖项满足《GB/T 36572-2018 电力监控系统网络安全防护导则》相关要求，应实现自身的安全，应安全、可控、可靠。 2、产品及其依赖项满足《GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求》3 级。
本体安全	1、产品及其依赖项满足《GB/T 36572-2018 电力监控系统网络安全防护导则》相关要求，应实现自身的安全，应安全、可控、可靠。 2、产品及其依赖项满足《GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求》3 级。 3、可限制仅特定地址登录；

指标项	具体要求
	4、远程管理设备时，应建立安全的通信协议；
硬件要求	硬件参数：规格：2U，CPU：≧64，内存：≧256 GB ，硬盘容量：≧48T，冗余电源，接口：2 千兆电口+6 万兆光口（接口允许通过扩展槽或配置探针设备满足要求），以上光模块满配，支持 ipv4 和 ipv6 双协议栈。 若单台设备性能不满足，允许配置探针设备达到性能要求。
性能要求	总体性能要求： 事件处理性能≧10000 eps（事件数每秒） 网络层吞吐≥30Gbps，应用层吞吐≥10Gbps 若单台设备性能不满足，允许配置探针设备达到总体性能要求
功能要求	实现以下功能的产品及其依赖项，均为本产品的供货范围。 1、支持高级威胁检测； 2、支持日志检索； 3、支持恶意代码检测； 4、支持从流量中发现威胁，如：协议异常、网络欺骗； 5、支持通过设备对流量进行抓包分析，可定义抓包流量双向或单向、数量、IP 地址、端口或协议类型； 6、支持告警的深度行为分析，行为包括 DNS 解析行为、TCP/UDP 交互行为、WEB 访问行为、传输文件行为； 7、支持暴力破解行为检测，检测内容包含：攻击者 ip、受害者 ip、使用协议、爆破次数、爆破成功与否等； 8、支持异常访问行为检测，检测内容包括：源 ip、违规访问者类型、主机名、访问类型； 9、支持识别爬虫行为并给出分析结果； 10、支持策略定义，可根据工作流进行处置动作定义，且能根据威胁等级、攻击结果、事件类别进行联动策略定义； 11、具备网络行为分析能力，实现对网络攻击特别是新型网络攻击行为的分析和告警；

7.1.4.3.15 国密服务器密码机

指标项	具体要求
兼容性	1、产品及其依赖项满足《GB/T 36572-2018 电力监控系统网络安全防护导则》相关要求，应实现自身的安全，应安全、可控、可靠。 2、产品及其依赖项满足《GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求》3 级。
本体安全	1、产品及其依赖项满足《GB/T 36572-2018 电力监控系统网络安全防护导则》相关要求，应实现自身的安全，应安全、可控、可靠。 2、产品及其依赖项满足《GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求》3 级。 3、可限制仅特定地址登录； 4、远程管理设备时，应建立安全的通信协议；
硬件要求	1、CPU 核数≥8，内存≥16GB，存储≥480G； 2、至少提供 4 个网络端口，2 个千兆电口，2 个万兆光口（满配光模块），

指标项	具体要求
	支持 ipv4 和 ipv6 双协议栈； 3、冗余双电源； 4、工作电压：220V（32V～343V）； 5、采用国家密码管理局批准的硬件芯片实现各类密码算法，保证算法的高安全性； 6、采用双路物理噪声源芯片产生高质量的真随机数作为密钥，保证密钥的安全产生； 7、配置备份恢复介质数量≥10； 8、配置国密 USB Key 数量≥10，USB Key 需要满足本次招标的智能密码钥匙技术参数；
功能要求	实现以下功能的产品及其依赖项，均为本产品的供货范围。 1、支持管理和应用的安全控制。 2、支持远程管理功能。 3、支持运行监控与日志审计。 4、安全关机功能。 5、支持国产 SM1/SM2/SM3/SM4 等算法。 6、支持对密钥的全生命周期管理功能，包括密钥生成、安全存储、备份恢复等功能。 7、采用国家密码管理主管部门批准的双物理噪声源芯片，提供多路随机源。 8、设备软件需符合 《GB/T 36322-2018 信息安全技术 密码设备应用接口规范》和《GMT 0018-2012 密码设备应用接口规范》要求。 9、具备授权控制机制、密码机操作身份认证应符合《GB/T 15843 采用数字签名技术》的认证要求。 10、重要的密钥操作采用多人分离管理机制。
性能要求	1、SM1 加解密：≥300Mbps； 2、SM2 签名：≥30000 次/秒； 3、SM2 验签：≥20000 次/秒； 4、SM3 摘要生成：≥500Mbps； 5、SM4 加解密：≥500Mbps。
资质要求	提供产品需具备由国家密码管理局商用密码检测中心颁发的商用密码产品认证证书，且证书中产品标准和技术要求的安全级别为符合《GM/T0028 密码模块安全技术要求》安全模块二级要求。

7.1.4.3.16 安全 U 盘

指标项	具体要求
兼容性	1、产品及其依赖项满足《GB/T 36572-2018 电力监控系统网络安全防护导则》相关要求，应实现自身的安全，应安全、可控、可靠。 2、产品及其依赖项满足《GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求》3 级。
本体安全	1、产品及其依赖项满足《GB/T 36572-2018 电力监控系统网络安全

指标项	具体要求
	防护导则》相关要求，应实现自身的安全，应安全、可控、可靠。 2、产品及其依赖项满足《GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求》3 级。
硬件要求	1、单个安全盘设备容量>=32G 2、产品接口 USB3.0
功能要求	实现以下功能的产品及其依赖项，均为本产品的供货范围。 1、整盘数据加密。 2、文件数据存储加密，采用国密 SM4 算法。 3、文件数据传输加密，防止通过 USB 监听手段窃取数据。 4、采用专用文件系统和文件浏览器进行文件管理；病毒、木马无法访问和感染设备存储区及文件系统。 5、支持用户设备身份注册绑定。 6、支持禁用、读取、写入、删除、修改等权限控制；支持内外网权限区分管理。 7、身份认证后才能登录安全存储设备。 8、口令错误超限后设备自动锁定。 9、支持口令长度和复杂性管理。 10、支持管理员对入网的移动存储介质进行注册，可以对已注册的移动介质进行管理，包括授权、启用、停用、删除、取消注册、导出注册列表等。 11、支持客户端自主申请移动存储介质注册，管理员统一对申请进行审批。 12、支持 U 盘与终端进行点对点的授权，可以灵活控制单个 U 盘在不同终端上拥有不同的使用权限。
性能要求	1、写入速度>=100MB/s。 2、读取速度通>=100MB/s。

7.1.4.3.17 杀毒 U 盘

指标项	具体要求
兼容性	1、产品及其依赖项满足《GB/T 36572-2018 电力监控系统网络安全防护导则》相关要求，应实现自身的安全，应安全、可控、可靠。 2、产品及其依赖项满足《GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求》3 级。
本体安全	1、产品及其依赖项满足《GB/T 36572-2018 电力监控系统网络安全防护导则》相关要求，应实现自身的安全，应安全、可控、可靠。 2、产品及其依赖项满足《GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求》3 级。
硬件要求	1、存储容量>=32GB。 2、接口类型 USB2.0 或 USB3.0。
功能要求	实现以下功能的产品及其依赖项，均为本产品的供货范围。 1、支持杀毒软件离线升级。

指标项	具体要求
	2、不会因为操作失误如删除、格式化，而把杀毒 U 盘变成普通的 U 盘。 3、可对载入的文件自动扫描，实现实时保护，避免病毒传播。

7.1.4.4 配套设备参数要求

7.1.4.4.1 卫星时钟

类别	指标参数
卫星时钟	支持双时钟源，包括双北斗授时。 时钟应能通过网络接口直接向局域网发布标准时间，各工作站运行相应对时进程，保持全网时钟同步。 时钟的误差应小于 1.0×10-6 秒。在时钟系统的操作面板上应显示年、月、日、星期、小时、分、秒。 具备不少于 2 光 2 电的网络接口，满配的光模块。电口支持千兆自适应及以上能力，光口支持万兆自适应及以上能力。 具备 IRIG-B 输入及输出光接口。 冗余双电源。 配天线（长度应可根据工程实际需求定制，长度 100-200 米） 系统通过竣工验收后，由原厂家提供 5 年免费上门维修服务。

7.1.4.4.2 运维终端

指标项	技术要求
处理器	8 核 2.3GHz 及以上，采用安全自主可控主处理芯片
内存	≥32GB
磁盘容量	固态硬盘 512G，机械硬盘 1TB
本机系统	含国产安全操作系统
输出分辨率	最高支持 2560*1440
生物识别	支持电容式指纹识别
蓝牙	蓝牙 4.2
I/O 接口	≥1*Type-C2.0 接口，≥2*USB3.2 Gen1，1 个 HDMI，1 个千兆网口
I/O 扩展	可通过扩展坞外接多个 USB 接口
电源输入	交流 100-240VAC/50-60Hz，
电源类型	外接型电源适配器
政府采购需求标准	应满足附件 3《政府采购需求标准》中对应投标产品形态的技术参数要求。

7.1.5 安全Ⅰ区

7.1.5.1 服务器技术要求

服务器主频均要求≥2.2GHZ。每台服务器配置≥2 路热插拔电源，每单路热插拔电源可满足设备满载运行要求，任意一路电源故障设备功能应不受影响。

服务器类型	配置
非 III 区服务器-容量型	1、2U 机架式服务器； 2、CPU: 配置≥2 颗安全自主可控 CPU；单颗 CPU 要求：X86 架构核数≥24，ARM 架构核数≥48 核； 3、内存：内存容量≥256GB，类型 DDR4 及以上，频率≥2933MHZ； 4、系统盘：配置≥960GB SSD【2*480GB SSD】硬盘； 5、数据盘：配置≥48TB HDD 物理容量（如：12 块 4TB 硬盘）； 6、RAID：配置 RAID 阵列卡，支持 RAID0/1/5/10 等主流 RAID 技术； 7、网络：配置≥2*双光纤端口 10GE 以太网卡（含光模块）； 8、电源：配置≥2 路热插拔电源，每单路热插拔电源可满足设备满载运行要求，任意一路电源故障设备功能应不受影响。
非 III 区服务器-通用型	1、2U 机架式服务器； 2、CPU: 配置≥2 颗安全自主可控 CPU；单颗 CPU 要求：X86 架构核数≥24，ARM 架构核数≥48 核； 3、内存：内存容量≥256GB，类型 DDR4 及以上，频率≥2933MHZ； 4、系统盘：配置≥960GB SSD【2*480GB SSD】硬盘； 5、数据盘：≥8TB HDD 物理容量； 6、RAID：配置 RAID 阵列卡，支持 RAID0/1/5/10 等主流 RAID 技术； 7、网络：配置≥2*双光纤端口 10GE 以太网卡（含光模块）； 8、电源：配置≥2 路热插拔电源，每单路热插拔电源可满足设备满载运行要求，任意一路电源故障设备功能应不受影响。

7.1.5.2 网络设备技术要求

本项目涉及的网络设备，中标方均应随主设备配置完整、满配的光模块，具体数量及技术选型以贵州电网公司实际需求为准。

7.1.5.2.1 万兆接入交换机

技术指标	要求
外观	机架式 1U 盒式交换机，前后通风
硬件架构	冗余电源；冗余风扇 满足安全自主可控要求，设备芯片采用安全自主可控
端口	≥48 口 SFP+万兆，≥6 口 QSFP40G/100G

性能要求	1.交换容量≥4.8Tbps，包转发率≥2000Mpps 2.支持≥4 台堆叠（IRF）/VSS，或者跨设备 LACP 聚合、LACP 边缘端口支持三层转发 3.所有端口支持巨帧转发（≥9216bytes） 4.10G、40G 端口支持路由口、路由子接口功能 5.端口支持 LLDP 功能 6.支持 IPv4/V6 双栈
二层功能	1.VLAN≥4K，支持 STP/RSTP/MSTP 2.支持 DHCPrelay，且 server 地址不小于 2 个 3.支持基于端口的广播风暴/组播/未知单播抑制 4. 支持 M-LAG 或 vPC 或 DRNI 等跨机箱链路捆绑技术
三层功能	支持 IPv4/v6 双栈支持静态路由、OSPFv2/v3、ISIS/v6、BGP/4+等动态路由协议 2.支持 ECMP 3.支持 IPv4/v6 三层组播：PIM-DM/SM,IGMP/MLD 4.支持 VRRP
VXLAN 特性	1.支持 Vxlan 协议，且支持 BGP EVPN 协议 2.支持 VXLAN over IPv6 3.支持 IPv6 VXLAN over IPv4 4.支持 VxLAN OAM: VxLAN ping, VxLAN tracert
网络管理	1.支持 POAP/Ansible/ZTP 等设备零配置自动化部署功能 2.支持 NETCONF 标准接口 3.支持 SNMP 通过域名方式访问 4.支持 NTP 客户端，支持时区修正，支持基于 IP 和域名访问 sever 5.支持 Console、Telnet 和 SSH2 命令行配置等网管方式 6.支持单物理端口和聚合组本地镜像、远程镜像 7.支持流量统计功能 8. 支持 ERSPAN
无损特性	支持 RDMA 和 RoCE（RoCE v1 和 RoCE v2） 支持 RoCE 流量可视：支持对 RoCE 流量 KPI 进行分析
安全服务	1.支持基本 ACL、扩展 ACL、基于时间 ACL 等安全防护技术 2.支持 AAA 认证，并支持用户分级管理和口令保护 3.支持设置 SNMPv3 加密 4.支持远程日志记录，指定记录服务器 IP 地址
配置	设备包含满配对应光模块；

7.1.5.2.2 千兆管理交换机

技术指标	要求
外观	机架式 1U 盒式交换机，前后通风
硬件架构	冗余电源；冗余风扇 满足安全自主可控要求，设备芯片采用安全自主可控

技术指标	要求
端口	≥48 口千兆电+≥4 个 SFP+万兆光，含满配对应光模块
性能要求	1.交换容量≥600Gbps，包转发率≥200Mpps 2.支持堆叠（IRF）/VSS，或者跨设备 LACP 聚合、LACP 边缘端口支持三层转发 3.所有端口支持巨帧转发（≥9216bytes） 4.10G、40G 端口支持路由口、路由子接口功能 5.端口支持 LLDP 功能 6.支持 IPv4/V6 双栈
二层功能	1.VLAN≥4K，支持 STP/RSTP/MSTP 2.支持 DHCPrelay，且 server 地址不小于 2 个 3.支持基于端口的广播风暴/组播/未知单播抑制
三层功能	1.支持 IPv4/v6 双栈支持静态路由、OSPFv2/v3、ISIS/v6、BGP/4+等动态路由协议 2.支持 ECMP 3.支持 IPv4/v6 三层组播：PIM-DM/SM，IGMP/MLD 4.支持 VRRP
网络管理	1.支持 POAP/Ansible/ZTP 等设备零配置自动化部署功能 2.支持 NETCONF 标准接口 3.支持 SNMP 通过域名方式访问 4.支持 NTP 客户端，支持时区修正，支持基于 IP 和域名访问 sever 5.支持 Console、Telnet 和 SSH2 命令行配置等网管方式 6.支持单物理端口和聚合组本地镜像、远程镜像 7.支持流量统计功能
安全服务	1.支持基本 ACL、扩展 ACL、基于时间 ACL 等安全防护技术 2.支持 AAA 认证，并支持用户分级管理和口令保护 3.支持设置 SNMPv3 加密 4.支持远程日志记录，指定记录服务器 IP 地址

7.1.5.3 安全设备技术要求

本项目涉及的安全及配套设备，中标方均应随主设备配置完整、满配的光模块，具体数量及技术选型以贵州电网公司实际需求为准。

7.1.5.3.1 网络终端接入核查设备

指标项	具体要求
兼容性	1、产品及其依赖项满足《GB/T 36572-2018 电力监控系统网络安全防护导则》相关要求，应实现自身的安全，应安全、可控、可靠。 2、产品及其依赖项满足《GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求》3 级。
本体安全	1、产品及其依赖项满足《GB/T 36572-2018 电力监控系统网络安全防护导则》相关要求，应实现自身的安全，应安全、可控、可靠。

指标项	具体要求
	2、产品及其依赖项满足《GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求》3 级。 3、可限制仅特定地址登录。 4、远程管理设备时，应建立安全的通信协议。
授权要求	支持≧1500 个终端数。
硬件要求	1、CPU 核数≧8；内存大小：≧32G，硬盘容量：≧960G。 2、配置冗余电源。 3、网络接口，配置≧（2 千兆电口+2 万兆光口），以上光模块满配。支持 ipv4 和 ipv6 双协议栈。 4、设备外形及安装：2U 及以下标准机架。
功能要求	实现以下功能的产品及其依赖项，均为本产品的供货范围： 1、支持扫描识别网络内的终端设备及类型并展示。 2、支持 802.1X：在网络接入层做准入认证、根据认证授权情况确定是否能访问网络。 3、支持 Portal：当新终端接入交换机时，交换机发现该终端未经身份认证，则将其浏览器请求重定向至 Portal 认证页面，用户通过身份认证成功后即可正常访问网络。 4、支持 MAB：启用此特性后，当通过 802.1X 认证的端口连接的设备是无法进行交互认证的设备时，交换机就会尝试使用基于 Mac 地址的免认证特性来识别客户端。 5、支持 SNMP 协议：可对外提供终端设备的 CPU 利用率，内存利用率，磁盘空间利用率、网络流量使用信息等信息，支持 SNMP trap 告警外发；支持 Syslog 协议外发日志。

7.1.5.3.2 蜜罐设备

蜜罐基于伪装欺骗技术，通过在攻击者入侵的关键路径上部署诱饵和陷阱，诱导攻击者进入与真实网络隔离的蜜网，让攻击者在蜜网中攻击伪装的服务、获取虚假的数据，进而完整记录攻击者行为，捕获高级未知攻击，并且对攻击者做取证和追踪溯源，为防守方提供先人一步的主动防御手段，保护真实资产，提升主动防御的能力。采用安全自主可控处理器及操作系统。

指标项	具体要求
兼容性	1、产品及其依赖项满足《GB/T 36572-2018 电力监控系统网络安全防护导则》相关要求，应实现自身的安全，应安全、可控、可靠。 2、产品及其依赖项满足《GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求》3 级。
本体安全	1、产品及其依赖项满足《GB/T 36572-2018 电力监控系统网络安全防护导则》相关要求，应实现自身的安全，应安全、可控、可靠。 2、产品及其依赖项满足《GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求》3 级。

指标项	具体要求
	3、可限制仅特定地址登录； 4、远程管理设备时，应建立安全的通信协议；
授权要求	蜜罐实例≥10；
硬件要求	硬件参数：规格：2U，CPU：≧16，内存：≧32 GB ，硬盘容量：≧2T，冗余电源，接口：2 千兆电口+2 万兆光口，以上光模块满配，支持 ipv4 和 ipv6 双协议栈，配套探针：≧4 台
功能要求	实现以下功能的产品及其依赖项，均为本产品的供货范围。 1、支持运行真实 ssh、telnet、Samba、Remote Desktop 服务的蜜罐，受到攻击后可以查询完整的连接建立与断开记录、用户密码登录记录、用户密钥登录记录、命令执行记录、文件遗留记录等 支持运行真实 MySQL、MongoDB、Redis、PostgreSQL、Memcached 服务的蜜罐，受到攻击后可以查询连接建立与断开记录和完整的数据库操作记录； 2、支持运行存在真实漏洞服务的蜜罐，包括 Struts2、PHP 等，并可以通过 POC 验证； 3、自定义蜜罐模板的用户名密码、数据库内容和标题等内容 4、支持运行学习真实 Web 类业务服务的蜜罐。蜜罐受到攻击后，可以查询完整的连接建立与断开记录和 Web 攻击记录 5、支持运行学习真实的基于 TCP 协议的业务服务的蜜罐。蜜罐受到攻击后，可以查询完整的连接建立与断开记录； 6、支持自定义添加多个蜜网，并且可以在蜜网内添加多个蜜罐服务，同一蜜网内的蜜罐可以互相连通； 7、探针可以自定义监听 1-65535 的任意端口 8、探针可以同时感知到使用 TCP 协议和 UDP 协议的探测 实时记录蜜罐访问流量； 9、系统服务蜜罐会记录蜜罐系统内 Bash 执行的系统命令及其参数，对不同的安全事件按威胁程度进行分级； 10、攻击者对 Web 服务蜜罐发起的攻击请求，蜜罐会智能识别其 payload 攻击类型和威胁等级； 11、探针感知探测后，可以查询完整的端口探测过程和探测中发送的数据，能够识别出扫描器的种类； 12、探针能感知到 Ping 扫描，被 Ping 后能够记录下 Ping 扫描源； 13、探针能够感知到 ARP 欺骗攻击，被 ARP 欺骗攻击后能够记录下攻击日志，至少包含被伪装的 IP、IP 伪装前的 MAC 地址和伪装后 MAC 地址； 14、支持展示在自定义时间内的入侵事件类型分布和攻击 IP 分布，并且以图表的形式呈现； 15、支持实时监控大屏，至少能够展示最近告警信息、入侵事件时间分布实时监控信息； 16、支持全局事件统计，能显示不同时间段的安全事件数量； 17、支持威胁 IP 排行和节点事件排行； 18、能够显示节点运行状态、节点是否部署，以及运行的服务类型等； 19、能够查看事件详情，至少支持连接异常、行为异常、文件变动等 20、能够对节点范围、事件类型、时间范围等进行精确查询统计；

指标项	具体要求
	支持以时间线的形式返回黑客入侵全过程，支持以视频的形式回放用户的命令行操作记录； 21、支持在感知到入侵信息和探测信息时，实时显示告警弹窗 支持对蜜罐入侵日志、端口探测日志进行处置，处置时支持输入处置记录； 22、显示已部署的蜜罐信息，包含蜜罐名称、当前状态、蜜罐服务信息。 23、支持通过管理界面实时监控探针运行状态，可以在管理节点上查看探针编号，对所有探针进行批量升级、绑定服务、解绑服务、修改探针类型等操作。能够查看指定探针的安全事件； 24、支持通过管理界面对不同探针关联不同蜜罐服务，且支持批量添加服务，同时可通过管理界面升级探针； 25、支持通过管理界面配置和下载外网（综合数据网等）诱饵和主机诱饵； 26、支持以邮件的形式实时告警。可告警内容包括蜜罐入侵事件、扫描事件、攻击者溯源事件、探针节点状态变化； 27、提供 API 二次开发接口，通过动态的 Token 进行身份验证； 28、支持密码、证书的认证方式； 29、支持配置账号锁定策略，如配置账号失败锁定次数和支持配置账号锁定时间； 30、支持可视化蜜罐网络拓扑，能展示管理节点、探针、蜜罐服务的连接关系，探针、蜜罐服务的运行状态，探针、蜜罐服务的威胁感知告警状态； 31、支持 SNMP 协议：可对外提供终端设备的 CPU 利用率，内存利用率，磁盘空间利用率、网络流量使用信息等信息，支持 SNMP trap 告警外发；支持 Syslog 协议外发日志。

7.1.5.3.3 堡垒机

指标项	具体要求
兼容性	1、产品及其依赖项满足《GB/T 36572-2018 电力监控系统网络安全防护导则》相关要求，应实现自身的安全，应安全、可控、可靠。 2、产品及其依赖项满足《GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求》3 级。
本体安全	1、产品及其依赖项满足《GB/T 36572-2018 电力监控系统网络安全防护导则》相关要求，应实现自身的安全，应安全、可控、可靠。 2、产品及其依赖项满足《GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求》3 级。 3、远程管理设备时，应建立安全的通信协议。
授权要求	支持≧1500 个资产。
硬件规格	1、CPU 核数≥8，内存≥32GB，存储≥4T。 2、网络接口，配置≧（2 千兆电口+2 万兆光口），以上光模块满配.支持 ipv4 和 ipv6 双协议栈。 3、设备尺寸≤2U 标准机箱。
安全及管理	1.配置国密密码卡，实现通信数据的机密性和完整性；实现访问控制信息和日志记录的完整性保护。

指标项	具体要求
	2.配置国密 USB Key 数量≥30，USB Key 需要满足本次招标的智能密码钥匙技术参数。 3.配置 CA 机构个人数字证书 10 套≥5 年授权。 4.支持审计日志自动、手动备份。日志最少保留 6 个月。 5.支持标准 SNMP 管理协议，支持 syslog 等标准日志格式外发。 6.实时监控系统 CPU、内存、磁盘的使用情况，支持 CPU、内存、磁盘使用超过阈值告警。
部署能力	1、支持 IPv6、IPv4 双协议栈。 2、物理旁路单臂部署，以逻辑网关方式工作；不改变现有网络结构。 3、单机部署、双机热备（HA）部署、分布式部署。 4、支持 B/S 运维。 5、支持 SNMP 协议：可对外提供终端设备的 CPU 利用率，内存利用率，磁盘空间利用率、网络等信息，支持 SNMP trap 告警外发；支持 Syslog 协议外发日志。
支持协议	1、字符协议：SSHv1、SSHv2、TELNET。 2、图形协议：RDP、VNC。 3、文件传输协议：FTP、SFTP、RDP 磁盘映射、RDP 剪切板。 4、协议代理审计模块：部署于 Liunx 服务器上，用于发布非标准协议或应用客户端并进行审计。
分权分域	1、系统内置系统管理员、审计管理员、安全管理员。 2、系统管理员可针对不同用户指定不同的管理权限，可设定用户（组）和资源（组）的管理范围。
用户管理	1、用户登录认证方式支持静态口令认证、手机动态口令认证、USB Key（数字证书）认证、AD 域认证、Radius 认证等认证方式；并支持各种认证方式和静态口令组合认证。 2、支持批量导入、导出用户信息。 3、支持用户手动添加、删除、编辑、设定角色、单独指定登录认证方式、设定用户有效期。 4、支持对用户指定限制登录 IP、登录时间段等规则。 5、支持口令有效期设置，用户账号口令到期强制用户修改自身口令。 6、支持登录控制台会话超时时间设置，用户在指定时间内无操作自动注销当前会话。 7、支持设定访问锁定策略，达到限制主账号密码输入错误次数和锁定时间的目的。
资源管理	1、支持服务器资源、网络设备资源、数据库资源、安全设备资源、C/S 资源、B/S 资源。 2、支持批量导入导出资源；支持手动添加、删除、编辑、查询资源。 3、支持资源的单点登录。
运维授权	1、支持一对一、一对多、多对多授权，如将单个资产授权多个用户，一个用户授予多个资产，用户组向资产组授权。 2、支持按授权名称、用户名称、用户账号、资源名称、资源地址、资源账号查询已授权信息。 3、支持在授权基础上设定双人复核登录，登录时必须经过第二人授权后才能登录。

指标项	具体要求
账号托管	1、支持定期变更目标设备真实口令。 2、支持密码策略设置。
审计日志	1、支持监控正在运维的会话，信息包括运维用户、运维客户端地址、资源地址、协议、开始时间等并可以实时阻断（支持命令黑名单和命令审批规则）。 2、对字符命令方式的访问可以审计到所有交互内容，可以还原操作过程的命令输入和结果输出。 3、图形资源访问时，支持键盘、剪切板、窗口标题、文件传输记录，并且对图形资源的审计回放时。 4、自定义审计查询条件，包括：时间范围、用户与用户 IP、资源 IP、命令关键字条件。 5、提供用户统计报表和系统运行报表并支持导出。

7.1.5.3.4 费控密码机

技术指标		指标参数
硬件设备	物理端口	标准机架式设备，应可放入 19 英寸标准机架，应至少包含以下端口： 电源端口、密码服务以太网端口、管理以太网端口、管理串口、打印口、密钥销毁触发装置。
	随机数发生器	随机数产生器应采用国家密码管理局批准使用的多片多路物理噪声源芯片
	可靠性	平均无故障工作时间应不低于 30，000 小时
	并发访问	>=2048
功能、性能、安全等要求	初始化功能	密码机应具备初始化功能，实现设备的原始状态到工作状态的转换。初始化操作应 至少包括设置设备主密钥、制作开机安全介质、制作授权安全介质、制作备份安全介质、设置设备参数、设置授权。 XX 密码机的初始化，除必须由厂商进行的操作外，系统配置、密钥管理、管理员管理等关键安全操作均应由用户方设备管理人员完成，密码机应提供图形化界面专用管理软件。
	密码运算	密码机应配用国家密码管理局认可的密码算法 SM1、SM2、SM3、SM4，采用硬件实现 SM1、SM2、SM3 和 SM4 算法。 SM1 算法加解密速率≥150Mbps SM2 算法签名速率≥6000 次/秒 SM2 算法验签速率≥4000 次/秒 SM3 算法运算速率≥700Mbps SM4 算法加解密速率≥700Mbps
	对称密码算法	密码机应配有 SM1 对称密码算法和 SM4 对称密码算法，SM1 密码算法的实现使用国家密码管理局指定的密码算法芯片，SM4 密码算法的实现遵循 GM/T0002-2012。

技术指标		指标参数
		对称密码算法的工作模式应至少包括 ECB、CBC、CFB 和 OFB 四种模式。
	公钥密码算法	密码机应配用 SM2 非对称密码算法，SM2 密码算法的实现遵循 GM/T0003-2012。
	密码杂凑算法	密码机应配用 SM3 杂凑算法，SM3 杂凑算法的实现遵循 GM/T0004-2012。另外，SM2 密码算法用于数字签名验签和计算消息认证码时，算法要求配用 SM3 杂凑算法，在 SM2 密码算法中使用的 SM3 杂凑算法的实现遵循 GM/T0004-2012。
	密钥管理	密码机应具备完整的密钥管理机制，密钥保护涵盖密钥的产生、注入、导入/导出、备份/恢复、查询和销毁整个生命周期，密码机必须保证密钥在生存周期的各个环节的安全性。密钥安全风险是指业务系统中的各种主控密钥和应用密钥在分发、保存、使用中的泄露、篡改、非法替换的风险。密码机应提供密钥安全性的设计保障。安全性设计应有明确的密钥保护措施和方法来消除密钥安全风险。
	访问控制	密码机应提供访问控制功能，防止非授权访问密码机引起的安全风险。访问控制包 括密码机的管理、使用和业务等方面内容
	管理要求	密码机的管理应提供图形化的专有软件进行管理，专有软件采用安全的方式与密码机连接，如采用信道加密的方法。密码机具备管理端口，管理端口与其他端口独立。管理端口是以太网口和串口。 采用串口管理模式应在通过安全控制检查后，采用人机接触的方式进行管理;采用以太网口管理模式应具有验证合法主机 IP 地址的功能，仅当口令认证通过后，方可进行管理工作。 密码机工作状态至少有两种：1）指令权限开放状态，该状态下，所有指令均可以使用，可以进行密钥的生成、注入、更新、导出等操作；2）指令权限受限的状态，该状态下，部分指令无法使用，无法进行密钥的生成、注入、更新、导出等操作。密码机指令权限开放状态和指令权限受限状态的转换应通过专有软件进行，转换过程中，应在授权安全介质（IC 卡、Key 等）接入的情况下进行。
	设备管理	在有远程集中管理需求时，密码机可具有设备远程集中管理功能，远程集中管理应 提供专用的图形化设备管理客户端软件
	安全性要求	密码机应具备国家密码管理局颁布的商用密码产品型号证书。 配置安全自主可控型号。
	安全服务要求	密码机通过密码服务命令报文对用户提供安全服务，实现安全功能。 密码机的底层软件应采用模块化设计，防止不同功能模块相互影响。密码机应通过技术措施防止用户的非法调用。 密码机的主机服务支持 TCP/IP 通讯模式。应用系统向密码机请求密码服务时，按指令 格式组合成正确的命令报文，发送给密码机，并等待接收密码机

技术指标		指标参数
		的应答报文。

7.1.5.3.5 运维区防火墙

类别	功能与技术描述
安全认证	满足国家安全产品有关认证要求。
产品架构	基于自主可控芯片的多核 CPU 架构
系统安全性	采用防火墙专用操作系统
	支撑系统不提供多余的网络服务
	系统不含任何高、中风险安全漏洞
冗余电源	提供双电源供电，并支持故障告警
设备支撑	配置设备机箱配套支架，设备高度不大于 2U
端口数量及类型	业务口要求：提供 2 个万兆光接口、8 个千兆光接口用于网络通讯，提供管理接口和 HA 端口。满配对应光模块
整机吞吐量	数据包吞吐量≥15Gbps
最大并发连接数	最大并发连接数≥300 万
每秒新建连接数	每秒新建连接数≥10 万
静态路由	最大静态路由条数≥1000 条
	支持基于源、目的 IP 地址的策略路由能力
访问控制策略	最大访问控制策略条数≥10000 条、最大地址集建立数目≥30000 条、最大服务集建立数目≥30000 条，最大域名对象数目≥3000 条
工作模式	1.支持透明模式
	2.支持路由模式
	3.支持混合模式
协议支持	1.支持 TCP、UDP 协议
	2.支持 IPv4、IPv6、ICMP、GRE（无需绑定物理接口）、VRRP、OSPF、BGP、RIP、SNMP 等协议
	3.支持 ARP、VLAN Trunk、QinQ 等协议
链路捆绑	1.支持多条链路的捆绑及链路间的负载均衡
NAT 功能	1.支持静态网络地址转换(Static NAT)
	2.支持动态网络地址转换(Dynamic NAT)
	3.支持网络地址及端口转换(PAT)
ALG 功能	1.能够识别常见应用协议并进行应用层处理
	2.支持对动态端口协议进行识别并控制
状态监测	1.支持基于会话的安全过滤，根据会话表放行或阻断数据包
	2.支持会话管理表，能够对特定的会话直接操作（删除等）
	3.支持会话超时保护，无报文的会话在一定时间后自动删除
流量及带宽管理	1.支持对 IP、IP 组、协议及端口进行带宽控制
	2.支持对最大与最小带宽进行限制
	3.支持根据 IP 地址限制并发 session 数量
连接控制	1、支持对源/目的地址对象、应用等设置并发和新建会话数量

	2、支持展示被拦截的 IP、地址对象、被拒次数、最近被拒时 间等信息
策略优化	1.支持分析失效、冗余、冲突的策略
	2.支持对策略有效性进行统计，支持策略的命中统计
	3.支持策略查询及导出功能
	4.支持批量修改策略配置信息，如批量禁用策略、批量删除 策略等
IPV6 功能	1.支持 IPv6 协议栈，支持 IPv6 地址的正确解析
	2.支持 IPV6 的 ACL 过滤
	3.支持 IPv6 的路由协议，包括 IPv6 的静态路由、动态路由（含 OSPFv3）和策略路由
	4.支持 IPV6 的状态检测功能
	5.支持 IPV6 的报文检测功能
	6.支持 NAT64、IPv4/IPv6 双栈
	7 支持 IPV6 DDOS 等攻击防护功能
	8.设备纯 IPv4 及纯 IPv6 的性能要求一致
攻击防御	1.支持对常见攻击方式进行检测与防御（DDOS、特殊报文、扫描攻击、特殊控制报文攻击等）
	2.抵抗各种典型的拒绝服务攻击，包括 SYN FLOOD，UDP FLOOD，ICMP FLOOD，IP 碎片包攻击，源 IP 地址欺骗攻击
	3.支持数据包的深度检测
	4.支持基于源及目的 IP 地址的并发连接数的控制
访问控制	1.支持基于域名的访问控制，且无需改变主机、终端的域名解 析配置
	2.支持基于 IP 地址的访问控制
	3.支持基于端口的访问控制
	4.支持基于协议的访问控制
	5.支持基于时间的访问控制
	6.支持基于连接的访问控制
	7.支持默认禁止策略
	8.支持用户自定义安全策略
黑白名	1.支持黑名单功能，被列入黑名单的 ip 及 ip 地址段，禁止所有访问，支持有效期设置，并提供黑名单增删 api 接口；黑名 单条码不少于 3000 条；
	2.支持白名单功能，被列入白名单的 ip 及 ip 地址段，放行所有访问，支持有效期设置，并提供白名单增删 api 接口；
IPSEC VPN	1.支持 IPSEC VPN。支持对隧道内流量进行监控
	2.支持多种（国际、国内）加密算法
应用控制	1．支持识别并控制各种常见应用
	2.支持自定义应用特征
入侵防御	1.支持告警和拦截非法、不正常、含攻击行为的报文
	2.支持手动自定义攻击规则库
	3.支持在线、离线、手动升级规则库
	4.至少支持威胁阻断模式、威胁监测模式
URL 过滤	1.支持黑白名单、恶意 URL 过滤
	2.内置恶意 URL 库，并支持在线、离线、手动更新

	3.支持自定义 URL 和阻断界面内容
	4．支持 URL 通配符，可通过通配符阻断某网站二级网站或页面
病毒过滤	1.支持对数据报文及文件进行病毒查杀
	2.支持对病毒报文及文件进行查杀、隔离等操作
	3.可拦截典型木马攻击行为
	4.支持在线、离线、手动更新规则库
管理方式	1.支持本地串口管理、远程管理、集中管理、分级管理等
	2.支持多主控台同时管理
	3.支持 HTTPS，SSH 等管理方式
	4.支持设置、查询和修改安全策略
	5.支持鉴别失败管理
	6.支持设备及策略集中管理
系统管理	1.支持自身状态监控，支持 snmp 管理，支持流量监测，提供支持设备状态监控、流量监控的北向 api 接口
	2.支持带外网管接口
	3.支持 Trap 协议
	4.支持配置备份、NTP 时间同步等
用户管理	1.支持对授权管理员的口令鉴别方式
	2.支持管理员权限划分
	3.支持对授权管理员、主机和用户进行身份鉴别
日志管理	1.支持流量日志、事件类日志、操作类日志、运行类日志及用户日志
	2.支持本地日志导出、日志清空、日志查询等
	3.支持 SYSlog 等方式发送至多个日志服务器，提供 syslog 范式化服务
	4.支持设置日志传输参数
行为审计	1.支持用户行为审计
	2.支持审计数据查询
自身安全性	1.支持配置限定用户登陆的 IP 地址范围
	2.支持 SSH、HTTPS 等加密方式进行远程访问
	3.支持对用户口令进行加密保存
	4.支持用户口令复杂度设置及检查
	5.支持最大登录失败重试次数设置
	6.支持用户登录超时时间设置
	7.支持双因子认证方式
	8.应保证所用的操作系统不存在安全漏洞
对外接口	1.设备应具备开放性、可扩展性，并提供开放接口，其中对外接口包括：允许策略增删改查、特征库版本、运行状态、策略命中情况等信息
	2.支持通过 SYSlog 方式以 UDP 发送日志对接监测系统，并可配合完成联动测试
可靠性与可用性	1.应提供 MTBF(Mean Time Between Failure)和 MTTR(Mean Time To Repair)指标，其中 MTBF 不小于 5 万小时，MTTR 不大于 2 小时
	2.支持电源冗余，电源冗余单元应支持热插拔功能

	3.支持软件防护加载、升级失败回滚
	4.支持 trouble-shooting 和性能监控、故障跟踪能力
	5.支持双机备份（双机热备、双机冷备）功能
	6.支持双机配置同步功能
	7.支持主备切换会话保持
	8.支持在关闭防火墙策略时，能够正常路由转发数据包
	9.支持设备状态监测、端口状态监测、链路连通性状态监测，可根据监测的设备状态，实现秒级的高可用切换，保障业务连续性
	10.应具有软件故障的监视功能，一旦软件出现死循环等重大故障时，应能自动再启动，并作出即时故障报告信息
供应链稳定性	具备供应链稳定性
售后服务	整机软硬件 5 年免费原厂维护、管理软件升级维护及技术支持服务（含特征库、规则库、许可等各种软件限制性的授权服务）

7.1.5.3.6 持续威胁检测与溯源系统（APT）

指标项	具体要求
兼容性	1、产品及其依赖项满足《GB/T 36572-2018 电力监控系统网络安全防护导则》相关要求，应实现自身的安全，应安全、可控、可靠。 2、产品及其依赖项满足《GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求》3 级。
本体安全	1、产品及其依赖项满足《GB/T 36572-2018 电力监控系统网络安全防护导则》相关要求，应实现自身的安全，应安全、可控、可靠。 2、产品及其依赖项满足《GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求》3 级。 3、可限制仅特定地址登录； 4、远程管理设备时，应建立安全的通信协议；
硬件要求	硬件参数：规格：2U，CPU：≧64，内存：≧256 GB ，硬盘容量：≧48T，冗余电源，接口：2 千兆电口+6 万兆光口（接口允许通过扩展槽或配置探针设备满足要求），以上光模块满配，支持 ipv4 和 ipv6 双协议栈。 若单台设备性能不满足，允许配置探针设备达到性能要求。
性能要求	总体性能要求： 事件处理性能≧10000 eps（事件数每秒） 网络层吞吐≥30Gbps，应用层吞吐≥10Gbps 若单台设备性能不满足，允许配置探针设备达到总体性能要求
功能要求	实现以下功能的产品及其依赖项，均为本产品的供货范围。 1、支持高级威胁检测； 2、支持日志检索； 3、支持恶意代码检测； 4、支持从流量中发现威胁，如：协议异常、网络欺骗； 5、支持通过设备对流量进行抓包分析，可定义抓包流量双向或单向、数量、

指标项	具体要求
	IP 地址、端口或协议类型； 6、支持告警的深度行为分析，行为包括 DNS 解析行为、TCP/UDP 交互行为、WEB 访问行为、传输文件行为； 7、支持暴力破解行为检测，检测内容包含：攻击者 ip、受害者 ip、使用协议、爆破次数、爆破成功与否等； 8、支持异常访问行为检测，检测内容包括：源 ip、违规访问者类型、主机名、访问类型； 9、支持识别爬虫行为并给出分析结果； 10、支持策略定义，可根据工作流进行处置动作定义，且能根据威胁等级、攻击结果、事件类别进行联动策略定义； 11、具备网络行为分析能力，实现对网络攻击特别是新型网络攻击行为的分析和告警；

7.1.5.3.7 入侵防御设备

指标项	具体要求
兼容性	1、产品及其依赖项满足《GB/T 36572-2018 电力监控系统网络安全防护导则》相关要求，应实现自身的安全，应安全、可控、可靠。 2、产品及其依赖项满足《GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求》3 级。
本体安全	1、产品及其依赖项满足《GB/T 36572-2018 电力监控系统网络安全防护导则》相关要求，应实现自身的安全，应安全、可控、可靠。 2、产品及其依赖项满足《GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求》3 级。 3、可限制仅特定地址登录。 4、远程管理设备时，应建立安全的通信协议。
硬件要求	硬件参数：规格：≤2U，CPU 核数：≧16，内存大小：≧16G，硬盘容量：≧1T，电源：冗余电源，接口：4 千兆电口+6 万兆光口，以上模块满配，支持 ipv4 和 ipv6 双协议栈。
功能要求	实现以下功能的产品及其依赖项，均为本产品的供货范围。 1、支持上传、下载、双向的文件内容过滤。 2、可准确地发现包括钓鱼攻击、恶意 SSL 证书、重定向攻击、获取权限、拒绝服务、漏洞利用等网络攻击行为。 3、提供统计分析面板，可将展示威胁统计、恶意 URL、恶意域名、恶意地址内容展示；并支持多时间维度筛选。 4、可在单条策略中启用病毒防护、入侵防御、网址过滤、文件过滤、文件内容过滤、终端过滤等安全功能选项。 5、支持安全策略的快速检索及基于名称、地址多维度的高级策略检索。 6、支持添加报表任务。生成可查看报表。 7、支持离线实现 IPS 特征库、威胁库更新。 8、访问控制规则支持模拟策略匹配，输入源目的 IP、端口、协议五元组信息，模拟策略匹配方式，给出最可能的匹配结果，方便排查故障，或环境

指标项	具体要求
	部署前的调试。 9、支持针对 HTTP、FTP 协议内容检测与病毒查杀。 10、设备具备独立的入侵防护漏洞规则特征库。 11、设备具备独立的热门威胁库，防护类型包括木马远控、恶意脚本、勒索病毒、僵尸网络、挖矿病毒等。 12、支持本地威胁情报检测和威胁情报库离线升级。 13 安全策略支持基于源安全域、目的安全域、源用户、源地址/地区、目的地址/地区、VLAN 等多种方式进行访问控制。 14、支持 SNMP 协议：可对外提供终端设备的 CPU 利用率，内存利用率，磁盘空间利用率、网络流量使用信息等信息，支持 SNMP trap 告警外发；支持 Syslog 协议外发自身日志。
性能要求	整机吞吐量>=10G； IPS 吞吐>=3G； 最大并发连接数不小于 200 万； 新建连接不小于 10 万/秒。

7.1.5.3.8 数据库审计

指标项	具体要求
兼容性	1、产品及其依赖项满足《GB/T 36572-2018 电力监控系统网络安全防护导则》相关要求，应实现自身的安全，应安全、可控、可靠。 2、产品及其依赖项满足《GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求》3 级。
本体安全	1、产品及其依赖项满足《GB/T 36572-2018 电力监控系统网络安全防护导则》相关要求，应实现自身的安全，应安全、可控、可靠。 2、产品及其依赖项满足《GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求》3 级。 3、可限制仅特定地址登录； 4、远程管理设备时，应建立安全的通信协议；
授权要求	数据库实例个数≥50;
硬件要求	硬件参数：规格：2U，CPU 核数：≧8，内存大小：≧16G，硬盘容量：≧4T，电源：冗余电源，接口：2 千兆电口+2 万兆光口，以上光模块满配，支持 ipv4 和 ipv6 双协议栈.
功能要求	实现以下功能的产品及其依赖项，均为本产品的供货范围。 1、支持对安全、自主、可控的数据库审计。 2、审计内容包括会话的终端信息、会话的主机信息、会话的操作信息等； 3、审计记录检索，支持通过访问来源信息（源 IP、业务主机端口、数据库名称、数据库用户、操作类型、表名、影响结果等、MAC 地址）方式进行检索； 4、查看日志详情，日志详情包括“时间、客户端 IP、目标数据库 IP、客户端 MAC、数据库类型、操作类型、客户端端口、响应时长、响应码、结果信息、客户端执行命令”等信息；

指标项	具体要求
	5、应用服务器对数据库的访问时，对数据库操作进行跟踪定位，包括数据库 SQL 执行情况、数据库返回值等。 6、会话回放，对用户从本次登录到退出这段时间内对数据库所做的所有操作按一定的时间间隔进行自动显示。 7、审计日志至少保留 180 天。 8、支持风险操作的实时监控及告警。风险信息包括“风险类型、风险次数、时间”等； 9、支持检测 SQL 注入及告警； 10、支持自定义风险规则。 11、支持 SNMP 协议：可对外提供终端设备的 CPU 利用率，内存利用率，磁盘空间利用率、网络流量使用信息等信息，支持 SNMP trap 告警外发；支持 Syslog 协议外发自身日志。
性能要求	1、SQL 审计处理能力≥10000/S。 2、吞吐流量≥2G/S。 3、检索亿级日志秒级响应

7.1.5.3.9 日志审计

指标项	具体要求
兼容性	1、产品及其依赖项满足《GB/T 36572-2018 电力监控系统网络安全防护导则》相关要求，应实现自身的安全，应安全、可控、可靠。 2、产品及其依赖项满足《GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求》3 级。
本体安全	1、产品及其依赖项满足《GB/T 36572-2018 电力监控系统网络安全防护导则》相关要求，应实现自身的安全，应安全、可控、可靠。 2、产品及其依赖项满足《GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求》3 级。 3、可限制仅特定地址登录； 4、远程管理设备时，应建立安全的通信协议；
授权要求	支持≧1500 个 IP
硬件要求	硬件参数：规格：2U，CPU 核数：≧8，内存大小：≧16G，硬盘容量：≧8TB，电源：冗余电源，接口：2 千兆电口+2 万兆光口，以上光模块满配，支持 ipv4 和 ipv6 双协议栈
功能要求	实现以下功能的产品及其依赖项，均为本产品的供货范围。 资产管理： 1、能够将资产按照多种维度进行分组、组织结构、业务系统等，提供便捷的添加、修改、删除、查询功能； 2、支持自定义资产类型； 3、支持对资产标签内容进行查询和管理。 日志收集： 1、Syslog、SNMP Trap 等协议被动采集日志；

指标项	具体要求
	2、支持文件读取、日志代理等方式主动采集； 3、支持 API 等方式交互式采集日志； 集中管控： 1、支持日志范式化和归一化； 2、支持按周期的方式对原始日志与范式化后的日志进行本地存储和外置备份； 审计管理： 1、支持对原始日志和范式化后的日志进行按条件检索； 2、支持对日志进行分析，生成告警信息，并发出通知。 3、可以对日志分析结果按条件进行检索。 日志转发： 1、支持 SNMP 协议：可对外提供终端设备的 CPU 利用率，内存利用率，磁盘空间利用率、网络流量使用信息等信息，支持 SNMP trap 告警外发；支持 Syslog 协议外发自身日志。 2、支持转发原始日志或归一化日志；
性能要求	1、日志处理总体性能≥2500EPS（事件数每秒）； 2、10 亿条日志量查询平均响应时间不超过 10 秒。

7.1.5.3.10 漏洞扫描

指标项	具体要求
兼容性	1、产品及其依赖项满足《GB/T 36572-2018 电力监控系统网络安全防护导则》相关要求，应实现自身的安全，应安全、可控、可靠。 2、产品及其依赖项满足《GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求》3 级。
本体安全	1、产品及其依赖项满足《GB/T 36572-2018 电力监控系统网络安全防护导则》相关要求，应实现自身的安全，应安全、可控、可靠。 2、产品及其依赖项满足《GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求》3 级。 3、可限制仅特定地址登录； 4、远程管理设备时，应建立安全的通信协议；
授权要求	支持≧1500 个 IP
硬件要求	硬件参数：规格：≤2U，CPU 核数：≧8，内存大小：≧32G，硬盘容量：≧4TB，电源：冗余电源，接口：2 千兆电口+2 万兆光口，以上光模块满配，支持 ipv4 和 ipv6 双协议栈
功能要求	实现以下功能的产品及其依赖项，均为本产品的供货范围。 1、支持动态发现 IT 环境中的资产； 2、支持手动录入资产；

指标项	具体要求
	3、支持主机资产的识别，同时获取资产存活状态、操作系统、端口、服务等信息。 4、兼容 CVE、CNNVD、CNVD 等主流漏洞库 ； 5、漏洞库支持离线升级。 6、支持常用及安全自主可控的系统漏洞、Web 漏洞、中间件漏洞、数据库漏洞、弱口令等发现能力； 7、支持扫描任务管理； 8、支持按需创建扫描任务，包括执行方式（包含立即执行、定时执行、周期执行）。 9、支持 SNMP 协议：可对外提供设备的 CPU 利用率，内存利用率，磁盘空间利用率等信息，支持 SNMP trap 告警外发；支持 Syslog 协议外发日志；
性能要求	1、支持主机漏扫并发 IP 数≧90。

7.1.5.3.11 国密服务器密码机

指标项	具体要求
兼容性	1、产品及其依赖项满足《GB/T 36572-2018 电力监控系统网络安全防护导则》相关要求，应实现自身的安全，应安全、可控、可靠。 2、产品及其依赖项满足《GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求》3 级。
本体安全	1、产品及其依赖项满足《GB/T 36572-2018 电力监控系统网络安全防护导则》相关要求，应实现自身的安全，应安全、可控、可靠。 2、产品及其依赖项满足《GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求》3 级。 3、可限制仅特定地址登录； 4、远程管理设备时，应建立安全的通信协议；
硬件要求	1、CPU 核数≥8，内存≥16GB，存储≥480G； 2、至少提供 4 个网络端口，2 个千兆电口，2 个万兆光口（满配光模块），支持 ipv4 和 ipv6 双协议栈； 3、冗余双电源； 4、工作电压：220V（32V～343V）； 5、采用国家密码管理局批准的硬件芯片实现各类密码算法，保证算法的高安全性； 6、采用双路物理噪声源芯片产生高质量的真随机数作为密钥，保证密钥的安全产生； 7、配置备份恢复介质数量≥10； 8、配置国密 USB Key 数量≥10，USB Key 需要满足本次招标的智能密码钥匙技术参数；
功能要求	实现以下功能的产品及其依赖项，均为本产品的供货范围。 1、支持管理和应用的安全控制。 2、支持远程管理功能。

指标项	具体要求
	3、支持运行监控与日志审计。 4、安全关机功能。 5、支持国产 SM1/SM2/SM3/SM4 等算法。 6、支持对密钥的全生命周期管理功能，包括密钥生成、安全存储、备份恢复等功能。 7、采用国家密码管理主管部门批准的双物理噪声源芯片，提供多路随机源。 8、设备软件需符合 《GB/T 36322-2018 信息安全技术 密码设备应用接口规范》和《GMT 0018-2012 密码设备应用接口规范》要求。 9、具备授权控制机制、密码机操作身份认证应符合《GB/T 15843 采用数字签名技术》的认证要求。 10、重要的密钥操作采用多人分离管理机制。
性能要求	1、SM1 加解密：≥300Mbps； 2、SM2 签名：≥30000 次/秒； 3、SM2 验签：≥20000 次/秒； 4、SM3 摘要生成：≥500Mbps； 5、SM4 加解密：≥500Mbps。
资质要求	提供产品需具备由国家密码管理局商用密码检测中心颁发的商用密码产品认证证书，且证书中产品标准和技术要求的安全级别为符合《GM/T0028 密码模块安全技术要求》安全模块二级要求。

7.1.5.3.12 安全 U 盘

指标项	具体要求
兼容性	1、产品及其依赖项满足《GB/T 36572-2018 电力监控系统网络安全防护导则》相关要求，应实现自身的安全，应安全、可控、可靠。 2、产品及其依赖项满足《GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求》3 级。
本体安全	1、产品及其依赖项满足《GB/T 36572-2018 电力监控系统网络安全防护导则》相关要求，应实现自身的安全，应安全、可控、可靠。 2、产品及其依赖项满足《GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求》3 级。
硬件要求	1、单个安全盘设备容量>=32G 2、产品接口 USB3.0
功能要求	实现以下功能的产品及其依赖项，均为本产品的供货范围。 1、整盘数据加密。 2、文件数据存储加密，采用国密 SM4 算法。 3、文件数据传输加密，防止通过 USB 监听手段窃取数据。 4、采用专用文件系统和文件浏览器进行文件管理；病毒、木马无法访问和感染设备存储区及文件系统。 5、支持用户设备身份注册绑定。 6、支持禁用、读取、写入、删除、修改等权限控制；支持内外网权

指标项	具体要求
	限区分管理。 7、身份认证后才能登录安全存储设备。 8、口令错误超限后设备自动锁定。 9、支持口令长度和复杂性管理。 10、支持管理员对入网的移动存储介质进行注册，可以对已注册的移动介质进行管理，包括授权、启用、停用、删除、取消注册、导出注册列表等。 11、支持客户端自主申请移动存储介质注册，管理员统一对申请进行审批。 12、支持 U 盘与终端进行点对点的授权，可以灵活控制单个 U 盘在不同终端上拥有不同的使用权限。
性能要求	1、写入速度>=100MB/s。 2、读取速度通>=100MB/s。

7.1.5.3.13 杀毒 U 盘

指标项	具体要求
兼容性	1、产品及其依赖项满足《GB/T 36572-2018 电力监控系统网络安全防护导则》相关要求，应实现自身的安全，应安全、可控、可靠。 2、产品及其依赖项满足《GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求》3 级。
本体安全	1、产品及其依赖项满足《GB/T 36572-2018 电力监控系统网络安全防护导则》相关要求，应实现自身的安全，应安全、可控、可靠。 2、产品及其依赖项满足《GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求》3 级。
硬件要求	1、存储容量>=32GB。 2、接口类型 USB2.0 或 USB3.0。
功能要求	实现以下功能的产品及其依赖项，均为本产品的供货范围。 1、支持杀毒软件离线升级。 2、不会因为操作失误如删除、格式化，而把杀毒 U 盘变成普通的 U 盘。 3、可对载入的文件自动扫描，实现实时保护，避免病毒传播。

7.1.5.4 配套设备参数要求

7.1.5.4.1 卫星时钟

设备类型	规格
卫星时钟	支持双时钟源，包括双北斗授时。 时钟应能通过网络接口直接向局域网发布标准时间，各工作站运行

设备类型	规格
	相应对时进程，保持全网时钟同步。 时钟的误差应小于 1.0×10-6 秒。在时钟系统的操作面板上应显示年、月、日、星期、小时、分、秒。 具备不少于 2 光 2 电的网络接口，满配的光模块。电口支持千兆自适应及以上能力，光口支持万兆自适应及以上能力。 具备 IRIG-B 输入及输出光接口。 冗余双电源。 配天线（长度应可根据工程实际需求定制，长度 100-200 米） 系统通过竣工验收后，由原厂家提供 5 年免费上门维修服务。

7.1.5.4.2 运维终端

指标项	技术要求
处理器	8 核 2.3GHz 及以上，采用安全自主可控主处理芯片
内存	≥32GB
磁盘容量	固态硬盘 512G，机械硬盘 1TB
本机系统	含国产安全操作系统
输出分辨率	最高支持 2560*1440
生物识别	支持电容式指纹识别
蓝牙	蓝牙 4.2
I/O 接口	≥1*Type-C2.0 接口，≥2*USB3.2 Gen1，1 个 HDMI，1 个千兆网口
I/O 扩展	可通过扩展坞外接多个 USB 接口
电源输入	交流 100-240VAC/50-60Hz
电源类型	外接型电源适配器
政府采购需求标准	应满足附件 3《政府采购需求标准》中对应投标产品形态的技术参数要求。

7.2 平台软件技术要求

7.2.1 安全Ⅲ区

7.2.1.1 云平台底座

云平台管控负责管理数据中心集群的物理资源，该系统将集群进行了整合，使得集群以一台超级计算机的形态展示在其他服务以及应用面前。在这台超级计算机之上提供弹性计算、关系型数据库、开放存储以及数据计算等服务，利用一个通用的云平台提供不同类型的云服务，满足应用系统不同场景的资源需求，为实现数据共享、打通信息孤岛提供了架构上的支撑。

云平台管控提供任务调度服务，是面向数据计算组件和大规模并行计算的底层基础

服务。任务调度能够自动检测故障和系统热点，重试失败任务，保证上层服务稳定可靠地运行。

云平台管控提供服务管理：提供计量、库存、权限、账户和审计等核心管理能力，实现云的可测量、多租户和按需自服务等关键特性。

云平台管控提供资源管理：对网络、计算设备和安全设备等物理资源统一管理的工具。对物理资源（包括计算存储设备、网络设备、安全设备等）和虚拟资源（虚拟化之后的资源池）的管理，包括对资源的注册、创建、销毁、回收等。

同时云平台管控服务控制分布式程序运行，隐藏下层故障恢复和数据冗余等细节，有效地提供弹性计算和负载均衡服务。其核心功能主要包括：分布式存储、任务调度、虚拟化、服务管理、资源管理以及远程过程调用等构建分布式系统常用的底层服务。

云平台底座总体描述及功能指标如下所示。

7.2.1.1.1 分布式云操作系统

指标子项	具体要求
文件系统	云操作系统应提供分布式文件系统，整合服务器的内置硬盘，屏蔽硬件故障，形成统一的分布式存储资源。分布式文件系统应支持多种数据存储方式
分布式存储	云操作系统应支持分布式存储的增量扩容和自动数据平衡能力
故障屏蔽	应采用多管理节点设计，避免集群单点失效，自动进行故障监测和数据迁移
任务调度	云操作系统提供分布式资源管理和任务调度框架，为上层云服务组件和应用提供跨服务器任务调度
可靠性	云操作系统应支持大集群规模，云平台集群规模最大应支持不少于5000 台物理服务器。
扩展性	应具备高可扩展性，可支持上亿个文件和 PB 以上量级的文件存储；支持不重启系统，增加物理服务器后自动扩容。
多租户	多租户技术可以实现多个租户之间共享系统实例，同时又可以实现租户的系统实例的个性化定制。通过使用多租户技术可以保证系统共性的部分被共享，个性的部分被单独隔离。 提供大数据分析能力给业务部门，不同业务部门可以通过多租户服务既共享大数据分析能力，同时保持一定的隔离性，互不影响。通过在多个租户之间的资源复用，运营管理维护资源，有效节省开发应用的成本。当共享资源进行升级时，所有租户可以同时升级。

7.2.1.1.2 运营管理

主要面向云资源的使用者及管理员，提供完整云平台运营能力，包括多级组织、角色权限、服务管理、计量计费等。以及基于用户的鉴权及资源分配，提供对云资源的各类操作、监控、分析、告警等管理功能。

指标子项	具体要求
大屏展示	支持云平台大屏展示，支持预置大屏和自定义大屏。自定义内容包括容量、性能、资源统计、告警等对象。全方位多维度实时展示平台运行和资源使用状态。 自定义大屏应提供可视化大屏在线编辑器，支持自定义数据来源，自定义每个内容的不同呈现形式（例如柱状图、饼图、仪表盘、地图等），支持拖拽方式，所见即所得，快速实现业务数据大屏的个性化定制。
用户管理	创建/修改/删除/启用/禁用/查询用户、修改/重置密码、角色授权、用户组管理、登录策略设置
角色管理	提供角色创建、修改、删除功能，支持自定义业务角色，设置角色所具有的操作权限，并将角色管理给相关用户；支持设置角色所能查看的具体云服务、操作项或资源。
登录策略管理	创建/修改/删除登录策略、支持白名单、关联用户、关联组织；支持按照登录时间和 IP 地址的白名单策略 支持设置能看见并使用这个登录策略的组织
菜单管理	支持创建、自定义、删除、启用、删除自定义菜单功能
服务管理	支持用户自定义服务目录，包括自定义云主机、云硬盘、网络等基础云服务、自定义组合的应用服务。支持应用服务发布，并支持在服务发布时关联审批流程。
计量计费	支持自定义计量计费报表，支持为不同服务配置不同的费率；可以查看各个组织的费用情况，并支持配置策略定期将费用报告发送到用户邮箱。

7.2.1.1.3 运维平台

运维平台作为云管理平台的核心功能组件，提供集中化的云平台运维能力。为 IT 管理人员提供云数据中心全面的资产管理，报表管理处理，各类资源及应用的维护和监控管理等功能。通过自动化和智能化技术，降低运维成本，提高运维效率。

指标子项	具体要求
集中化运维	平台具备集中化的运维管理能力，提供集中监控、资源拓扑、日常运维、运维分析、系统管理等能力，实现物理设备到应用的全方位监控，收集并展示运维对象的告警、日志等信息，同时提供报表、大屏、自动化以及运维数据分析能力，提升运维效率。
资源管理	平台提供配置管理数据库管理能力，支持对平台中物理设备（包括但

指标子项	具体要求
	不限于机柜、服务器、网络设备、存储设备）、虚拟资源的集中管理。支持关联关系查询、资源对象的变更记录管理，支持对资源库中的资源进行增、删、改、查、合并等常用操作，支持自定义资源管理对象类型。
告警管理	支持集中管理系统中物理设备（服务器、存储、网络设备）和虚拟资源的告警信息。
	支持告警清除、指派、调整级别、设置告警提示音等功能。
	支持告警转发能力，系统可按照管理员指定的远程通知规则，将不同类型告警通过短信、邮件发送给不同用户、用户组进行处理。
容量管理	支持资源容量分析。用户可按照不同维度（数据中心、不同资源池、不同主机组/集群）查看计算、存储、网络资源的使用情况和分配情况。支持提供容量趋势预测，评估已有资源消耗进度和时间。
	支持资源闲置分析，支持根据具体的业务需求，设定需要的闲置资源判定规则。针对每个云服务器和块存储给出缩容建议。支持预估资源优化后可节约的资源量，预测资源利用率提升比例。
	支持资源瓶颈分析，支持根据具体的业务需求，设定需要的瓶颈资源判定规则。针对每个云服务器和块存储给出扩容建议。预估资源优化需要多少资源量。
应用监控	支持运维人员进行应用监控与分析。支持将应用与对应的资源对象进行关联。通过对应用关联的资源对象性能指标以及告警进行综合评估，实现应用监控。
	应用的部署节点信息支持动态更新，虚拟机的横向扩展和动态迁移等变更可以自动反映到应用监控关联拓扑中。
自动化运维	支持用户自定义运维脚本，包括 shell、python 等脚本。支持将运维脚本批量下发到指定虚拟机、计算节点、管理节点并执行，简化重复性大的运维管理工作。
	提供自动化的平台日常巡检管理，支持创建自定义巡检任务，支持日常巡检和升级前巡检，日常巡检支持实时任务、定时任务、周期任务，支持导出巡检报告，报告包含巡检任务的基本信息、检查结果和处理建议等。
报表管理	支持容量、资源、设备统计、资源利用率、告警统计等报表。支持报表自定义呈现，管理员可对已有指标进行重新组合、过滤以实现自助式业务分析。支持通过表格和图表的方式进行统计报表展示。支持配置定期生成报表。

7.2.1.2 基础设施服务

7.2.1.2.1 弹性计算

7.2.1.2.1.1 云服务器

云服务器提供一种处理能力可弹性伸缩的计算服务，它的管理方式比物理服务器更简单高效。根据业务需要随时创建实例、扩容磁盘或批量删除多台云服务器实例。

云服务器是一个虚拟的计算环境，包含 CPU、内存等最基础的计算组件，是云服务器呈现给每个用户的实际操作实体。云服务器实例是云服务器最为核心的概念，可以通过云服务器管理控制台完成对云服务器实例的一系列操作。

指标子项	具体要求
云主机网络管理	支持为云服务器指定 IP 地址创建云主机，方便运维人员进行 IP 的统筹管理，支持配置 IPv6/IPv4 双栈网络，云主机实例可自动获取 IPv6 地址进行内网通信。
云主机管理	支持云主机生命周期管理和维护，包括但不限于创建、启动、关闭、重启延期云主机到期时间，其中创建、启动、关闭、重启、延期应支持批量操作，提升管理员操作效率。
云主机监控	支持对云主机 CPU、内存、硬盘等基础指标进行监控，为用户提供系统级、主动式、细粒度监控服务。
镜像	支持对云主机的系统盘和数据盘创建整机镜像模板，支持在租户界面可以制作包含系统盘和数据盘的镜像，提供操作系统、预装的公共应用及用户的私有应用和用户业务数据，可用于快速发放包含用户业务数据的新弹性云主机。 应提供虚拟机镜像、快照完整性校验功能，防止虚拟机镜像被恶意篡改。
虚拟负载均衡	支持负载均衡服务，负载均衡服务基于软件方式实现，不依赖于特殊硬件设备。可以将用户业务访问流量自动分发到多台云服务器，扩展应用系统对外服务能力。
调度策略	支持云主机不同的调度能力。根据云主机组的不同策略，组中的云主机可以分散在不同的物理主机上，可以提高业务的可靠性。
热迁移	支持虚拟机热迁移，虚拟机在不中断业务的情况下实现从一台计算节点迁移到同一个资源池内的另外一台计算节点上。。
云主机高可用	支持云主机高可用，当某台物理节点发生意外故障，在其上运行的云主机能够在其他正常的物理节点上重新启动，保障业务的连续性。支持防群体性故障高可用，防止虚拟机被攻击反复引起的故障传染
数据备份	支持用户通过快照对云主机的数据进行备份，通过快照进行云服务器的数据恢复。
安全组	支持安全组服务，可以对进出虚拟机端口的网络报文进行安全过滤规则设置。虚拟机端口与安全组关联后，安全组规则可对进出虚拟机端口的网络报文进行过滤，只有规则允许的报文可通过。安全组规则修改后立刻生效，针对修改规则前已处于连接状态但不满足更新后的安全规则的链接可立即阻断。
登录云主机	支持多种云主机登录认证方式，包括密钥登录、密码登录、VNC 登录，方便云服务器的配置、管理等操作
磁盘挂载	单个云主机能够挂载不低于 16 块数据盘，单个数据盘的存储容量不小于 32TB
分散部署	云服务器支持分散部署： 1.云服务器支持严格分散、尽量分散两种部署策略； 2.同一组云服务器支持基于不同宿主机，不同机架、不同交换机分散

指标子项	具体要求
	部署。

7.2.1.2.1.2 容器服务

容器服务是一种高性能可伸缩的容器管理服务，支持企业级 Kubernetes 容器化应用的生命周期管理。

容器服务简化集群的搭建和扩容等运维工作，整合虚拟化、存储、网络和安全能力，是云端最佳的容器化应用运行环境。

容器服务支持企业级容器化应用的生命周期管理，可高效地在云端运行容器化应用，实现自动化、智能化、简单高效的应用管理和运维。

指标子项	具体要求
持久化存储的备份和还原	支持基于云盘的快照和恢复功能。
权限管理	通过控制台为子账号配置对应的 Kubernetes 集群内 RBAC 权限，并提供常用的默认权限如管理员、运维人员、开发人员等。
命名空间和配额管理	支持对命名空间的 CPU、内存、存储等资源设置配额。
容器网络策略管理	支持容器隧道网络和 VPC 网络两种网络模式，其中 VPC 网络支持与云主机网络直接互联互通。
路由管理	支持容器服务权重配置，使流量按比例分发
配置管理	支持对应用的保密字典进行集中定义和管理，保密字典支持 Opaque、私有镜像仓库登录密钥、 TLS 证书等类型。
YAML 编排	支持使用 yaml 文件创建应用，查看已部署应用的 YAML 文件，可修改已部署 yaml 配置。
多集群管理	支持多集群的统一管控。
容器伸缩	支持手动伸缩和弹性伸缩，支持手工调整 Pod 的副本数量进行横向伸缩，支持配置容器资源阈值进行容器实例的自动伸缩。 支持 HPA 弹性伸缩策略，实现 POD 水平自动伸缩的功能。 支持增强弹性伸缩策略，包括基于 CPU 利用率、内存利用率和实例数百分比等指标进行弹性扩缩容，支持设置最小步长
容器存储管理	支持从页面上进行容器存储卷（本地存储、块存储、文件存储、对象存储）的生命周期管理。
容器实例远程控制	容器实例支持以 remoteshell 工具方式进行远程访问控制。
日志管理	支持日志采集，对容器的标准输出日志和应用日志文件进行采集，并支持自定义 Tag，方便进行日志统计和过滤等分析操作。
白屏化编排	支持页面对资源进行编排，资源包括：Deployment、StatefulSet、DaemonSet、Job、CronJob 等。

指标子项	具体要求
监控	支持集群、节点、应用、容器实例层面的监控，支持集成 Prometheus 服务的能力，为集群提供全方位监控大盘。
节点伸缩	支持从 Web 页面一键式手工自助添加和删除节点，伸缩过程中无需人工干预。支持通过弹性伸缩组自动创建工作节点并加入集群。支持设定缩容规则触发后自动下线工作节点。 支持节点池管理，方便对一组节点进行批量编辑和配置管理，提升用户管理效率。 支持基于 CPU、内存等指标策略或者定时周期策略进行集群资源节点弹性伸缩。
节点区域支持	支持工作负载节点跨可用区统一管理。
节点类型支持	支持 GPU 类型节点、支持裸金属服务器。
集群创建/删除	容器服务与云平台无缝对接，能够通过控制台实现集群的一键式自助创建和删除集群。
集群操作审计	支持查看 Kubernetes 集群中的事件整体概览以及重要事件（访问、命令执行、删除资源、访问保密字典等）的详细信息。支持查看 Kubernetes 集群中常见的计算资源、网络资源以及存储资源的操作统计信息。操作包括创建、更新、删除、访问。支持查看 Kubernetes 集群中某类资源的详细操作列表；支持自定义时间维度查询。
集群概览	提供平台看台功能，能够快速查看资源的总体运行状态，包括节点、组件、应用的运行状态，集群的事件记录以及集群的当前的资源使用情况。
Matser 节点高可用	Master 节点高可用支持 5 节点和 3 节点模式，5 节点模式下故障 2 台，3 节点模式下故障 1 台，不影响集群正常使用，全部 Master 节点全部故障时，不影响已有业务正常使用。
Worker 节点高可用	Worker 节点故障迁移时，故障节点上 POD 自动迁移。
高性能调度器	支持大数据场景批量作业生命周期管理，支持多种主流作业模板统一调度，包括 MPI、Tensorflow 等。支持多种高级调度策略，提升作业调度效率和资源分配率；支持 pod 延迟创建，提升容器集群的并发处理能力。

7.2.1.2.1.3 容器镜像服务

容器镜像服务是面向容器镜像、配置管理组件（Helm Chart）等符合开放容器标准（OCI）的云原生制品安全托管及高效分发平台。支持便捷的容器镜像权限管理、容器镜像同步分发等能力，便于进行容器镜像全生命周期管理。容器镜像服务简化了注册中心的搭建及运维工作，并联合容器服务等云产品，降低交付复杂度。

适用于开发运维一体（DevOps）持续交付、自动同步镜像等场景使用。

指标子项	具体要求
制品支持种类	支持容器镜像、HelmChart 等 OCI 制品。
制品生命管理	提供高可用的容器制品管理服务，支持制品的上传、下载、删除等功能。
容器镜像的安全托管	提供镜像仓库管理功能，支持命名空间和镜像仓库分级管理，支持公共或私有镜像仓库，其中公共仓库可被系统所有用户访问，私有仓库只能被有权限的用户访问。
权限控制	支持按照组织架构和项目维度的权限管理，支持子账号权限管理。
触发器策略设置	支持对容器镜像仓库创建触发器，支持全部触发、表达式触发、Tag 触发等方式，支持触发器访问记录的查看。
镜像信息查看	支持容器镜像版本的查看，包括镜像的摘要信息、镜像大小、最后更新信息、层信息等。
镜像跨账号同步	支持跨账号场景，支持手动触发某个镜像版本的同步；同时支持基于同步规则，支持镜像推送后自动同步。
镜像跨地域同步	支持跨地域镜像同步场景，支持手动触发某个镜像版本的同步；同时支持基于同步规则，支持镜像推送后自动同步。
集成能力	可与容器服务深度集成，在容器服务平台部署应用，支持免密拉取配置，避免每次设置 secret，支持可视化选择镜像仓库及版本。

7.2.1.2.1.4 弹性伸缩

弹性伸缩服务可根据用户的业务需求和预设策略，自动调整计算资源，使云服务器数量自动随业务负载增长而增加，随业务负载降低而减少，保证业务平稳健康运行。用户可根据业务访问量的变化，配置伸缩策略，通过弹性伸缩服务控制伸缩组中云服务器的数量，进行扩容和减容操作，从而保证服务正常运行。

指标子项	具体要求
监控告警	支持实时统计伸缩组内指标数据，并在统计值满足告警条件时触发告警，自动执行伸缩规则，动态调整伸缩组内的云主机的实例数量，监控指标包括但不限于 CPU 使用率、内存使用率、内网出流量、内网入流量等。
伸缩策略	为有效应对业务浪涌，需要支持虚拟机弹性伸缩服务，用户可以自主配置业务系统弹性伸缩策略，弹性伸缩策略支持如下几种： (1) 在特定的时间触发； (2) 按固定的周期触发； (3)根据业务系统的业务压力（告警，如 CPU 利用率，内存利用率，网络流入/流出速率）触发。
自动加载	支持根据配置的伸缩规则弹性扩张云主机实例，配置自动扩容出来的云主机的登录方式以及自动扩容的云主机是否使用负载均衡来进行流量转发。

7.2.1.2.1.5 资源编排

资源编排服务是一项简化云计算资源管理的服务。资源编排服务定义的模板规范编写资源栈模板，在模板中定义所需的云计算资源、资源间的依赖关系等。资源编排服务的编排引擎将根据模板自动完成所有资源的创建和配置，实现自动化部署及运维。

资源编排提供作业管理，自定义配置操作参数和执行脚本、管理执行目标以及存储参数文件的平台。构建丰富的运维操作库，如内置批量修改操作系统缺省用户密码、批量为操作系统打补丁的日常操作，标准化各种运维场景。并通过编排管理向管理员提供将运维操作库的单个操作，通过图形化的方式编排组合的能力，更大程度上满足各业务场景的自动化运维操作。

指标子项	具体要求
图形化编排	提供资源编排组件，支持通过图形化界面对云服务进行编排。在模板中可以定义所需资源间的关联关系、资源配置等，如云服务器、 容器、弹性伸缩等，帮助用户简化云计算资源管理和自动化运维的服务。
服务模板	支持新建模板，也可以导入已有的模板，基于服务模板可以快速构建服务并上线到服务目录。
易用性	支持在线查看资源编排服务支持的资源类型及各资源类型详情。

7.2.1.2.2 存储服务

7.2.1.2.2.1 块存储

块存储服务是一种基于分布式架构的、可弹性扩展的虚拟块存储设备。可以在线进行操作，使用方式与传统服务器硬盘完全一致，可以对挂载到云服务器上的云硬盘做格式化、创建文件系统等操作，并对数据持久化存储。同时，块存储服务具有更高的数据可靠性，更高的 I/O 吞吐能力和更加简单易用等特点，适用于文件系统、数据库或者其他需要块存储设备的系统软件或应用。

指标子项	具体要求
自主可控	为保障自主可控，分布式存储软件需国产自研并拥有自主知识产权和软件著作权登记证。
系统架构	采用全对称分布式架构，无独立元数据节点；支持 X86 架构存储节点和 arm 架构存储节点。
副本策略	支持多副本、EC 的数据保护模式。
负载均衡	存储集群池内节点间和盘间容量负载均衡，支持标准 SCSI 和 iSCSI 协议访问存储池。
快照	支持卷的快照和回滚，支持秒级快照。

指标子项	具体要求
重删压缩	可基于业务负载情况，进行自适应重删压缩，且重删压缩后的性能损耗低。
在线变规格	支持在不中断业务的前提下，在线变更云盘规格，满足灵活多变的业务需求。
指定集群	支持存储集功能。在创建云盘时，可以指定云盘落在特定集群。
在线扩容	支持在线扩展容量，扩容期间无需关闭虚拟机，无需卸载云盘；系统盘在线扩容不停业务；支持横向扩展能力；单集群最大可扩展至≥256节点。
运维管理	支持用户自定义性能图表并指定对象，对 CPU 利用率、内存利用率、带宽、IOPS 、时延、卷容量利用率、存储池利用率等进行统计。
加密	数据加密：支持块服务开启数据加密功能。 国密加密：支持 SM4 国密加密算法。 加密盘：支持 AES 256 和国密加密。
可靠性	单节点故障情况下，IO 归零时长小于 10 秒。 支持数据快速重构，当磁盘或存储节点故障时，系统能自动进行数据重建，在无人工干预条件下，数据重建速度能满足：每 TB<15 分钟。

7.2.1.2.2.2 对象存储

对象存储是提供的安全、低成本、高可靠的云存储服务。相比传统自建服务器存储，对象存储在可靠性、安全性、成本和数据处理能力方面都有着突出的优势。使用对象存储，可以通过网络随时存储和调用包括文本、图片、音频和视频等在内的各种非结构化数据文件。

对象存储将数据文件以对象（Object）的形式上传到存储空间（Bucket）中，提供键值对（Key-Value）形式的对象存储服务。可以根据 Object 的名称（Key）获取该 Object 的内容。

指标子项	具体要求
接口协议	对象存储服务支持 RESTful API 接口、兼容 Amazon S3 接口，通过开发工具包 SDK 或直接通过 RESTful API 进行基础和高级对象存储操作，提供 key-value 键值对形式的对象存储服务
功能要求	支持对象的简单上传、追加上传、下载、删除、列举、复制，获取对象的元数据、创建多段上传任务。 支持列举存储空间、创建存储空间、删除存储空间、列举存储空间内对象、获取存储空间的元数据。
	支持将存储空间配置成静态网站托管模式，并通过存储空间域名访问该静态网站。支持防盗链，支持设置基于 HTTP header 中表头字段 Referer 的防盗链方法。
	支持生命周期管理、定义和管理存储空间内所有对象或对象的某个子集的生命周期。

指标子项	具体要求
	bucket 以及 object 支持设置标签，可以基于标签设置访问权限和数据生命周期管理策略
	支持一朵云跨可用区、跨地域之间的异步远程复制。
	支持多个集群使用统一域名对外提供服务
	支持存储清单功能，支持根据配置的清单生成规则，生成清单报告并存储到指定的存储空间内。
	支持定时上传，定时上传任务，按照每天/每周/每月或自定义的频率自动上传本地磁盘或目录中的文件到对象存储系统。
	支持文件语义，提供 POSIX 文件语义 bucket 和客户端。
安全性	支持客户端加密功能，可以使用客户端加密 SDK，在本地进行数据加密，并将加密后的数据上传到对象存储，既支持云平台密钥管理系统托管的用户主密钥，也支持用户自主管理的密钥。 支持服务器端的加密功能，用户能够使用密钥管理系统上创建的密钥进行加密。可以使用国密算法对 bucket 内保存的数据以及单独 object 进行加密存储。

7.2.1.2.2.3 虚拟机备份服务

虚拟机备份服务包括云服务器的配置规格，系统盘和数据盘的数据，利用备份数据恢复云服务器业务数据，最大限度保障用户数据的安全性和正确性，确保业务安全。

功能子项	具体要求
云服务器备份	支持云服务器备份数据的管理，支持用户在云管界面通过云服务器备份数据进行恢复，可以将备份数据恢复到原服务器或者恢复到新的指定服务器；支持删除不需要的备份数据；支持用户自主搜索自定义时间内的备份数据
虚拟机应用备份	支持备份服务，用户可以自助申请对虚拟机或者虚拟机应用进行备份服务，支持用户自助配置备份策略，包括指定备份周期、执行时间点、备份策略有效期、副本保存策略（需要保留的副本数或者副本保留时间）、全备/增备策略等，用户可以选择特定策略进行手动备份，或者按照策略规则自动备份。

7.2.1.2.3 网络

7.2.1.2.3.1 负载均衡

负载均衡是将访问流量根据转发策略分发到后端多台云服务器的流量分发控制服务。负载均衡扩展了应用的服务能力，增强了应用的可用性。负载均衡通过设置虚拟服务地址，将添加的同一地域的多台云服务器实例虚拟成一个高性能和高可用的后端服务池，并根据转发规则，将来自客户端的请求分发给后端服务器池中的云服务器实例。

负载均衡默认检查云服务器池中的云服务器实例的健康状态，自动隔离异常状态的云服务器实例，消除了单台云服务器实例的单点故障，提高了应用的整体服务能力。负载均衡的应用场景为高访问量的业务，提高应用程序的可用性和可靠性。典型应用场景：高访问量的业务、扩展应用程序、消除单点故障、同城容灾、跨地域容灾。

指标子项	具体要求
总体要求	负载均衡服务采用通用服务器架构实现。提供 4 层 TCP/UDP 和 7 层 HTTP/HTTPS 协议类型的服务。
架构要求	负载均衡支持 IPv6，支持挂载 IPv4 或 IPv6 的后端应用服务器。
功能要求	七层负载均衡模式下支持配置域名或者 URL 转发策略，将来自不同域名或者 URL 的请求转发给不同的云服务器处理。
	支持用户在负载均衡上创建监听器，支持四层、七层的监听策略。支持配置监听器的监听协议/端口，支持四层以及七层协议。
	支持负载的加权轮询算法、加权最少连接、源 IP 算法等分配策略；支持 IP 地址、HTTP cookie、应用程序 cookie 等会话保持策略。
	支持 NAT64 和 NAT46 功能，实现 IPv4 转 IPv6 或 IPv6 转 IPv4 能力。
	支持用户为监听器配置健康检查策略，用于检查后端服务器的状态，支持四层以及七层检测方式，并可以设置检查周期、检查超时时间、重试次数等。 对于七层 HTTP/HTTPS 协议，支持设置协议与后端服务器交互的方法、服务器响应的状态码以及 URL。

7.2.1.2.3.2 专有网络

专有网络是独有的云上私有网络。可以完全掌控专有网络，例如选择 IP 地址范围、配置路由表和网关等，可以在自己定义的专有网络中使用云资源如云服务器、云数据库和负载均衡等。可以将专有网络连接到其他专有网络或本地网络，形成一个按需定制的网络环境，实现应用的平滑迁移上云和对数据中心的扩展。

专有网络是完全隔离的虚拟网络环境，配置灵活，可满足不同的应用场景；部署主动访问公网的应用程序；跨可用区容灾；业务系统隔离；构建混合云。

指标子项	具体要求
总体要求	支持用户创建自己的专有网络，同时支持自定义配置 IP 地址、子网、路由表 。支持不同 VPC 之间的安全隔离。
功能要求	支持批量申请弹性 IP 地址，可以自行选择弹性 IP 地址所属的地址池、分配方式（自动分配或者手动分配）等策略。
	用户可以独立配置自己的网络环境，包括自助创建子网（IPV4、IPV4&IPV6）、指定子网网段/网关/掩码、子网使用的 DNS 等参数，支

指标子项	具体要求
	持为子网中的云服务器配置静态路由。
	支持 VPC 流日志能力，能够提供 VPC 内网络安全日志查询能力：记录安全组/网络 ACL 流量日志，查询被允许/拒绝的策略匹配的日志情况。
	支持不同 VPC 间互通，支持 VPC 内的云服务器通过专线与线下数据中心的服务器互通要求。
	支持创建 IPv4 NAT 网关，支持 SNAT 和 DNAT 配置，用于支持 NAT 网关绑定多个地址。
	支持用户可以创建网络 ACL 配置入向/出向规则，进行网络访问控制功能，从而实现对一个或多个子网流量的访问控制。

7.2.1.2.3.3 NAT 网关

NAT 网关是一款公网网关，提供 NAT 代理（SNAT 和 DNAT）功能，具有 10 Gbps 级别的转发能力和跨可用区的容灾能力。NAT 网关作为一个网关设备，需要绑定公网 IP 才能正常工作。创建 NAT 网关后，可以为 NAT 网关绑定弹性公网 IP。

NAT 网关适用于专有网络类型的云服务器实例主动访问公网和被公网访问的场景，例如：搭建访问公网服务的 SNAT 网关；搭建提供公网服务的 DNAT 网关。

支持 NAT 网关实例创建、修改和删除，每个 NAT 网关实例可配置 SNAT 规则和 DNAT 规则。

7.2.1.2.3.4 VPN 网关

VPN 网关是一款基于外网（综合数据网等）的网络连接服务，通过建立加密通道的方式实现企业本地数据中心、企业办公网络或外网（综合数据网等）终端与专有网络之间安全可靠的私网互联。

VPN 网关常见应用场景：建立专有网络与本地数据中心之间的连接；建立专有网络与专有网络之间的连接；建立专有网络与客户端之间的连接；建立客户端和站点之间的连接。

指标子项	具体要求
IPSEC VPN	支持 IPSEC VPN 服务，支持 IPsec-VPN 建立专有网络（VPC）到本地数据中心的 VPN 连接
SSL VPN	支持软件 SSL VPN 服务，支持通过 SSL-VPN 功能远程接入 VPC，修改 SSL 服务端的名称、本端网段、客户端网段信息，支持创建 SSL 客户端证书，支持 AES128、AES192、AES256 加密算法，支持国密算法和证书认证。

7.2.1.2.3.5 专有云 DNS

专有云 DNS 是运行在专有云环境的一套 DNS 产品，为企业内网环境（专有云网络）提供域名解析服务。专有云 DNS 通过设置域名与 IP 地址的对应规则和策略，可以将来自客户端的域名访问请求重定向到云平台中的云产品资源上、云平台中的自建业务应用上、企业内网的业务系统上、外网（综合数据网等）服务提供商的服务资源上等。

指标子项	具体要求
总体要求	VPC 私有域名转发配置管理和解析：当 VPC 内云服务器访问内网域名时，内网 DNS 直接对内网域名进行解析，向云服务器返回对应被访问的云服务器的私网 IP 地址。当 VPC 内云服务器访问外网域名时，内网 DNS 会将对外域名的解析请求转发外网 DNS 进行解析。
功能要求	支持域名管理，支持创建/删除/修改域名，支持域名关联 VPC（专有网络）。
	支持记录集管理，支持创建/删除/修改记录集，支持 A、CNAME、MX、TXT、PTR、SRV、NS、SOA 类型记录集。
	内网权威域名管理和解析：支持 IPV6 域名解析服务
	支持一个域名可以关联多个 VPC（专有网络），方便统一管理部署，减少管理员的配置工作。

7.2.1.2.4 云桌面

云桌面将电脑的主机、CPU、硬盘等硬件设施都集中在云端，用户只需要将超轻量的终端连接到电视机、屏幕等主流显示设备上，就可以连接云桌面，访问各种应用和文件。 云上电脑不但具备传统电脑的所有能力，而且具备超越传统线下电脑的能力，例如动画渲染、制图设计、软件研发等对计算性能要求非常高的工作场景。

指标子项	具体要求
总体要求	支持本地身份认证、UOS 域控，同时必须能支持对接统一身份访问管理平台
	提供自主知识产权的桌面云软件。
	支持基于国产自主产权芯片（包括不限于鲲鹏/海光等芯片）服务器部署，支持采用一套桌面云架构部署和管理国产操作系统多种资源池。
	支持主流的服务器、存储厂商设备，并提供兼容性清单；支持集中式 SAN 存储和分布式存储架构。
	支持用户终端至虚拟桌面的运行界面以屏幕变化量的方式传送给客户端显示，无外设接入的情况下，网络上仅传输屏幕变化指令和客户端输入设备的指令。

桌面部署	支持统信 UOS、银河麒麟操作系统。
	支持完整克隆专有模式桌面（重启、关机后保留个性化设置、个人数据），以及链接克隆还原模式桌面（重启、关机后，桌面恢复到初始状态，不保留个人数据）；支持用户和虚拟桌面之间采用一对一、多对一、多对多的分配方式，提供从独占资源到共享资源池的桌面使用模式；国产桌面均可支持以上分配模式。
	支持在不依赖显卡的情况下 4K 分辨率的超高清显示，支持多显示器扩展
	支持用户直接在虚拟机设置桌面的分辨率，无需切换到终端本地修改，且支持客户端系统显示缩放比设置重定向到虚拟桌面，保留用户原有习惯。
	支持临时桌面发放，在发放桌面时，可对桌面进行有效期设定；有效期到期后自动将桌面进行桌面使用权限回收。
	支持虚拟桌面内置视频播放器，实现视频流重定向到终端侧解码，降低服务器资源消耗，支持主流视频格式。
	支持多个池化桌面资源合并成一个大资源池。
终端接入	支持多种类型终端登录桌面云，支持瘦终端、利旧 PC 终端及移动终端设备。支持 ARM 芯片以及鲲鹏、兆芯等国产芯片，支持国产统信 UOS、银河麒麟等操作系统。
	支持统信 UOS、麒麟等 PC 利旧并且支持 PC 终端锁定功能，屏蔽本地开始菜单和资源，只能用于访问桌面云。
	支持开机自启动和联动关机功能，打开终端电源可以直接登录虚拟桌面，关闭虚拟机可联动关闭本地终端。
	支持单终端同时登录多个桌面，在不断开连接的情况下，实现多桌面的快速切换。
	支持双屏双桌面，每个屏幕呈现不同的桌面，共用一套终端及键鼠设备。
	支持客户端实时帧率显示和网络状态显示，网络时延及丢包数统计。
	支持广域网优化能力，保证极端网络条件下（时延 150ms、丢包 1%、抖动 40ms）的桌面使用效果。
	支持用户登录时弹出提醒功能，弹出内容可由管理员自定义。
	支持管理员在管理平台统一设置每日提醒功能，终端用户在登录时可查看相应的信息提醒，便于企业安全信息宣贯传递。
	支持同时对接多套不同域控制器（包含国产域控、本地域控），用户一次登录认证即可访问登录所有域控下的用户桌面
	支持一套桌面云管理系统实现用户从内网、外网访问桌面时获取不同桌面资源，以实现安全管控。
	支持双网隔离模式，可配置内外网站点登录地址，当终端网络发生切换时，终端能够自动检测并切换登录地址。
	支持终端通过代理服务器访问桌面，在终端无法和桌面直接连通的组网场景下，允许配置桌面云客户端代理，通过代理服务器进行流量转发。
管理运维	支持用户在桌面出现异常时，远程关闭、重启、强制关闭、强制重启自己的桌面
	支持用户自助维护通道和检修工具，当桌面云出现登录异常时，用户可以通过自助维护通道登录，使用检修工具对网卡状态、桌面代理、IP

	地址、系统时钟、桌面服务状态、虚拟机注册状态等进行检查，并支持自动修复。
	支持用户自助快照和恢复功能，用户可以在登录界面对虚拟机磁盘进行自助备份管理及快照恢复。
	支持虚拟桌面快速部署功能，一次任务完成虚拟机 CPU/内存/磁盘容量/网卡/显卡规格配置、指定 IP 地址、虚拟机命名、加入域/OU、指定所属权限组，任务完成后，用户可以直接访问桌面，无需管理员干预。
	支持定时任务创建虚拟桌面和重建虚拟桌面，避免业务高峰期占用系统 IO 资源。
	支持批量电源管理功能，管理员可启动/关闭/重启/休眠/强制关闭/强制重启虚拟桌面。
	支持远程会话管理，管理员可远程断开、注销用户会话； 支持管理员给用户批量发送消息。
	支持自动会话管理，管理员可定义在无鼠键输入消息时虚拟桌面自动锁屏/断开/注销/重启/关机操作，时长可设置。
	支持批量在线增加 CPU/内存规格，重启虚拟机生效；支持在线增删虚拟网卡、在线扩容磁盘的功能，立即生效。
	支持删除用户桌面，支持在有效时间内可以对删除的用户桌面进行恢复。
	支持定时任务功能以实现自动化运维，支持定时开机防止启动风暴、长时间未使用的桌面自动关机释放资源、长时间未注销的桌面自动休眠、长时间异常的虚拟机自动重启，时长可设置；定时任务支持指定时间或按天、按周、按月周期性执行。
	支持系统管理员在管理平台对用户桌面执行一键收集日志；用户终端日志可在客户端进行一键日志上报，进行自动收集上传，便于故障快速定位。
	支持虚拟桌面重建系统盘、还原系统盘功能，可立即执行或虚拟桌面 下次启动时生效，可以保留系统盘作为数据盘；
	支持将虚拟桌面设置为维护模式，当进行系统升级时可防止用户误登录。
	支持远程协助功能，管理员可发起协助请求，用户同意后可查看、操作虚拟桌面。
	支持桌面云代理自动升级，可配置管理员强制更新、管理员通知更新、用户自助更新。
	支持所有桌面云基础架构组件状态监控与告警、执行健康检查
	支持自定义集群、主机、虚拟机的 CPU/内存/磁盘/网络阈值，根据重要程度分为提示告警、次要告警、重要告警、紧急告警，支持邮件订阅。
	可提供桌面云系统告警与状态监控管理功能，且支持对接第三方 SMNP 平台，便于运维人员进行故障定位，保证系统稳定运行。
	支持将管理员操作日志上传到第三方的 syslog 服务器，便于系统管理员进行统一的日志管理，满足安全审计要求。
	桌面云管理系统支持集权管理和三员分立管理模式。集权管理可获取超级管理权限；三员分立包含系统管理员、安全管理员、安全审计员，不同用户权限相互制约，无超级管理员。

	支持桌面发放时指定用户的权限组，针对已发放的桌面，管理员可对单个或批量用户桌面权限组进行灵活变更
	桌面云管理系统支持本地账号和 AD 域账号，支持限定用户只能从指定 IP 段和时间段登录，支持配置密码复杂度和条件锁定策略。
	支持区域管理，可指定区域管理员，该用户仅能管理自己区域的虚拟桌面，可指定区域最大可容纳的 CPU 个数、内存大小、存储容量、桌面数量；且区域属性支持对镜像模板，计算机组，桌面组，应用组，应用服务器组，用户/用户组、协议策略功能等对象应用
	支持查看、条件筛选、导出操作日志，日志不可修改、删除，事后溯源。
策略管理	支持策略管理功能，管理员可以统一配置外设、音频、多媒体、显示、文件/剪切板、接入控制、会话、带宽、水印、鼠标键盘等策略；支持将策略应用给不同的对象类型，包括但不限于虚拟机、桌面组、用户、用户组、OU 等，以提供灵活精细的桌面管理。
	支持对外设实现精细化管控，允许或阻止 USB 接口、并口、串口类设备重定向到虚拟桌面，可按扫描仪、摄像头、打印机、U 盘、USB-Key、蓝牙、无线网卡等设备类型控制。
	支持外设黑白名单，可按设备 PID/VID、设备 class 类型允许或阻止某一款设备重定向到虚拟桌面。
	支持显示等级控制，可配置显示帧率、视频帧率、图像和视频压缩参数，网络优时优先保障显示清晰度，网络差时优先保障流畅度。
	支持桌面通道带宽控制，可对总带宽、显示、USB、串口、打印机、摄像头、文件/剪切板等通道进行限速，确保有限带宽场景下优先保障流畅度。
	支持用户从内网、外网访问桌面时获取不同策略，如内网登录时可以使用 U 盘，外网登录时禁用所有外设。
统计报表	支持在统一的桌面管理平台批量筛选查询，可以根据虚拟桌面计算机名、ID、操作系统版本、用户名、IP、运行状态、登录状态、创建时间段、所属区域等进行筛选，支持模糊查询，支持数据导出。
	支持报表形式直观展现运行状态（运行，关机，休眠）、登录状态（使用中，断开连接，未注册）、分配状态（已分配，未分配，不可分配）统计系统中桌面使用情况，支持数据导出。
	支持在统一的桌面管理平台提供用户登录行为日志查询和审计功能，支持记录计算机名、ID、终端 IP/MAC 地址、操作系统、终端主机名、登录时间、断开时间，支持数据导出。
	支持在统一的桌面管理平台提供用户在线趋势分析、用户使用时长、未使用的虚拟桌面分析，支持数据导出。
系统安全	支持设置用户首次登录时强制修改密码、定期修改密码、图形校验码、双因素认证等安全策略，确保用户身份安全。
	支持通过 IP（段）、MAC（组）、时间段等方式限定用户只能从指定终端/时间登录；支持证书认证，未导入证书的 BYOD 设备无法登录。
	支持用户和 MAC 地址绑定功能，限定用户只能从指定 MAC 终端登录，支持 PC/TC 终端及移动终端。支持手工录入、批量导入以及首次登录时自动绑定（可维护排除用户）。
	支持虚拟桌面 IP 和 MAC 自动绑定功能，一旦修改 IP 桌面将无法访问网络，防止 ARP 仿冒攻击。

	支持虚拟桌面普通删除和安全删除功能，安全删除将对物理磁盘写零擦除，保证用户数据不被窃取、不被恶意利用。
	支持互联网接入的桌面云网关。支持负载均衡、认证转发、协议加密等功能；网关支持高可靠和横向扩展的能力。
	支持桌面云网关 CPU/内存利用率、接收/发送流量、TCP 报文重传比、在线用户数统计，支持按用户维度的接收/发送流量、最大流量、RTT 往返时延统计。
	支持用户登录位置发生变化时，提示上次用户登录客户端地址和登录时间。
	支持水印功能，提供固定位置和随机运动两种显示模式，可配置颜色、字体大小、条数、倾斜度以及自定义显示内容，且对桌面虚拟机以及云应用均支持。
	支持终端与虚拟桌面文件/文件夹、剪切板传输，支持只读（只进不出）、只写（只出不进）、读写（双向）模式。
	支持模板克隆出来的虚拟桌面自动随机化默认管理员账号密码、自动清理本地用户组中非必要的用户（组）账号，降低安全风险。
高可用/扩展	支持动态池模式下，管理员自定义高峰期和低峰期时间段，针对不同时间段可以设定桌面池内预启动的云桌面数量，来提升用户的登录使用体验。
	支持配置虚拟桌面蓝屏时自动重启、关闭或 HA 到其他主机。
	支持集群负载均衡调度策略，可根据 CPU、内存资源占用率触发调度任务，虚拟机启动时动态选择、运行时自动迁移到低负载主机，实现资源的自动负载均衡。
	支持虚拟桌面在不同主机、存储 LUN 之间热迁移，虚拟桌面迁移过程业务不中断。
	支持各基础架构组件之间具备高可用健康监控、自动故障切换能力，无需其他外界组件或人工协助。用户在获得 VDI 桌面连接后，单个组件故障将不会影响用户使用。
	支持配置管理虚拟机互斥功能，以确保提供相同功能的组件运行在不同物理主机上，确保平台高可用。
	支持管理数据（数据库/日志/证书文件等）自动备份功能，也可备份到第三方 FTP 服务器，支持定时备份和立即执行备份。
	支持网络闪断桌面自动重连功能，当出现网络不稳定导致桌面闪断后能自动重连，无需用户重新输入密码，且重连次数、间隔可由管理员统一配置。
	架构组件基于访问层、控制层、资源层，采用松耦合架构，可分层配置各基础架构组件服务器高可用方案及横向、纵向扩展，单套桌面云管理系统可同时管理的在线桌面数量≥10000。

7.2.1.3 数据库服务

7.2.1.3.1 分析型数据库（AP 库）

分析型数据库用于打通大数据生态，支持对 PB 级数据进行高并发、低延时的分析处理，可以与主流的 BI 工具（如 Tableau、帆软等）轻松连接，开展 BI 可视化分析或者即席查询。支持实时数据，支持高并发实时写入与更新，写入速度可达亿级 TPS，数据写入即可查。支持海量数据复杂查询，全并行计算，实现 PB 级数据关联分析亚秒级响应。支持海量数据点查询，提供 PB 级存储，每秒亿级记录写入与查询。支持联邦查询无缝对接离线批量计算平台，无需移动数据，直接交互式分析，快速获取查询结果。可以直接单独查询数据仓库（如：HIVE 等）的表数据，也可以与实时数据结合进行联合计算。数据库软件须具备自主知识产权，符合国家相关政策标准，采用安全自主可控软件，满足安全、自主、可控的要求。

指标子项	具体要求
总体要求	应满足附件 3《政府采购需求标准》中对应投标产品形态的技术参数要求。 提供交互式分析型数据库服务，兼容 PostgreSQL 协议，与大数据生态无缝连接，支持高并发和低延时地分析处理 PB 级数据。 提供生产环境下支持的最大单集群规模，包括节点数、总存储容量、总记录数等信息的材料。
功能要求	具备数据生命周期管理功能，过期数据系统自动清理
	支持图形化 SQL 客户端编辑工具，提升 SQL 开发效率，客户端工具能力至少包括：对象浏览，语法高亮，格式智能化，自动填充等功能。
	支持值（List）、区间（Range）表分区，可以将 TEXT、VARCHAR 以及 INT 类型的数据作为分区键（Partition Key）
	支持基本数据类型：boolean、tinyint、smallint、int、bigint、float、double、decimal、varchar、date、time、timestamp。
	支持数据按行存储或按列存储，提供面向海量数据进行多维分析与多表关联分析的能力，同时也支持高并发明细点查询。
	支持离线数仓的批量导入；支持流计算实时入库；同时数据也支持导出至对象存储。
安全性	具备完善的权限认证，支持多级租户管理机制，多层账号管理体制，子账号管理。
兼容性/开放性（接口、引擎等）	支持标准 SQL 语法（DDL，DML）

7.2.1.3.2 事务型关系数据库（TP 库）

指标子项	具体要求
总体要求	应满足附件 3《政府采购需求标准》中对应投标产品形态的技术参数要求。 事务型关系型数据库，同时支持 x86 和 ARM 计算架构，提供高吞吐强一致性事务处理能力、高可用能力、大数据高性能查询能力 数据库软件须具备自主知识产权，符合国家相关政策标准，避免潜在的产权纠纷。 采用安全自主可控软件，满足安全、自主、可控的要求。 支持国产操作系统部署数据库。
功能要求	支持标准的 SQL92/SQL99/SQL2003/SQL2011 规范，包括 DML、DDL、DCL 和常用数据库对象等。
	能够实现复杂的数据操作，例如 FROM 子查询、WHERE 子查询、嵌套子查询、常用聚合函数及分组、排序等操作等。
	支持各种场景下的数据库对象，包括但不限于表、视图、存储过程、触发器、函数、JSON、游标等。
	具备快速在线 DDL 机制，不因在线 DDL 引起在线交易阻塞或业务中断。
	多语言支持，多语言支持，包括中文和英文等，能够支持简体中文、繁体中文、英文等多种字符集（例如：GBK、UTF-8、UTF-16、Unicode 等），能够使用这些字符集存储数据
	支持常用的数据类型，包括数值数据类型、字符串数据类型、日期时间类型等类型；支持其他数据类型，包含但不限于数值型、布尔型、JSON 型、大字段/二进制类型（BLOB）等。
	支持常见的数字操作函数、转换函数、字符函数、日期/时间函数、安全函数、窗口函数、聚合函数等。
	支持多表 JOIN，多表关联查询等数据库基础功能，对应用透明。 支持数据库函数的运算和结果集的合并运算，如：UNION、INSERT INTO SELECT、COUNT（DISTINCT）、GROUP BY、SUM、COUNT、MAX、MIN 等。
	含有完善的优化器设计，实现高效的 SQL 在线优化，保证在复杂 SQL 场景下的查询效率，同时需做到对应用无中断，无感知。 支持 hint 等方式手工执行的方式。
	兼容 SQL：2011 的常用语法，支持存储过程、函数、视图等
	支持表空间管理，表空间用于管理数据对象，与磁盘上的一个目录对应
	支持 Json 数据类型，方便存取常见的 Json 数据格式
	支持大对象类型，包括 clob、text、blob 类型，其中 text 和 blob 支持最大 1G
	支持多种分区表类型，包括但不限于范围分区、哈希分区、列表分区、间隔分区等；支持组合分区，如可以实现列表、范围组合分区等；支持分区键包含多列；支持增加、删除、合并、拆分、交换、截断、重命名等分区操作；支持分区表迁移。
	支持存储过程、自定义函数和包 PACKAGE
	支持多种触发器
	具备良好的 SQL 兼容性，支持 ANSI/ISO SQL89、ANSI/ISO SQL 92、

指标子项	具体要求
	ANSI/ISO SQL 99、ANSI/ISO SQL 2003、ANSI/ISO SQL 2011 标准。
	支持服务器端错误自动重试，故障不中断业务。
	支持可编程的 SQL 语言，包括但不限于存储过程、函数、外部函数、过程包和触发器等，用于实现复杂的判断和运算功能。
部署架构	支持主备形态集群模式，支持基于裸机或云主机形态进行部署，为不同业务场景提供灵活的部署形态选择。部署模式支持读写并行或读写分离部署模式。
	数据库集群需具备高效的故障自动处理能力，支持故障自动切换和故障自动重加入，集群系统能够检测到故障并进行自动切换。数据库集群支持 7*24 小时长时间不间断运行。
	读写并行部署时，支持数据库集群规模可达 2 个及以上节点，集群每个节点均支持读写同时进行且保障多节点间的缓存一致性；集群具备多节点负载均衡能力，数据库集群各节点间的资源能够负载均衡，以提高设备利用率，充分发挥硬盘高速读写性能、网络高速传输性能，防止负载集中出现的服务器性能瓶颈。
	读写分离部署时，支持数据库集群规模可达 2 个及以上节点，支持原生只读实例和读写分离功能，可支持不少于 2 个只读实例，自动实现读写分离以及读节点间的负载均衡，保障多节点间数据强一致性。
	数据库的系统架构需要有容错性设计，当主节点发生进程异常、网络异常、操作系统异常、磁盘等异常无法提供服务时，备节点能够自动启用并接管服务，在整个架构上提供系统的高可用。
	支持机房级别的故障容灾能力，机房故障时同城机房能够提供持续服务能力。
	支持版本不停机在线升级和回退，升级和回退期间业务平稳。
	支持逻辑和物理备份功能。
安全性	支持完善的安全防护能力，包括全密态加密、透明加密、SSL 加密、动态脱敏、国密算法
	支持 SM4 国密算法
	支持用户权限、细粒度权限控制
兼容性	兼容主流 Oracle 语法，数值类型（整数、序列、浮点…）、字符、日期、二进制、JSON/JSONB、XML、LOB、自定义类型（CREATE TYPE）；数据库对象，系统函数，高级包等
可用性&可靠性	支持表级闪回查询，闪回查询支持索引
	细粒度物理备份恢复，包括库表级备份恢复
	集群采用多节点冗余架构，无单点故障。

7.2.1.3.3 内存数据库

内存数据库是兼容 Redis 协议标准的数据库服务，基于双机热备架构及集群架构，可满足高吞吐、低延迟及弹性变配等业务需求，内存数据库用于多样化存储的场景：存储数据库使用；缓存加速应用访问。

指标子项	具体要求

指标子项	具体要求
总体要求	兼容 Redis 协议标准、提供可靠的缓存数据库服务，基于双机热备架构及集群架构，可满足高吞吐、低延迟等业务需求
功能要求	集群兼容性高，支持 string，hash，list，set，sortedset 等常见类型，支持事务和订阅
	提供多种规格的缓存数据库实例，支持实例的创建、重启、释放、备份等管理操作，支持清除全部数据和清理过期数据；支持实例的网络隔离
	支持主从、集群等不同形态，支持规格大小变更
	支持缓存分析，支持大 key 分析、热 key 分析
可靠性	同时支持 RDB（Redis Database Snapshot）和 AOF（Append Only File）以及持久化机制，支持设置 AoF 落盘开关，保障数据丢失最小化
	支持实例的手动和自动备份，支持自动备份策略设置，支持主从、集群版等多种形态实例的原地恢复，克隆实例，支持备份集下载
	支持分钟级粒度监控，支持自定义监控项，包括基础监控（cpu，内存，qps，命中率，keys，expiredkeys 等）、string，hash 等常见类型监控，事务，订阅等监控
安全性	内存数据库内核和 OS 层经过专业安全加固，可用性 99.95%
	支持域名访问，支持端口号修改，避免默认端口号扫描风险
	支持多账号，支持设置读写、只读权限，最小化授权提供更高安全保障
	支持白名单设置，提供灵活的安全访问管理能力
性能要求	主从版可支持不少于 64GB 缓存容量，集群版可支持不少于 1TB 缓存容量，集群版可支持不少于 128 个分片节点，当一套不支持本项目所需的内存库存储规模时，需提供多套，以满足项目需求。

7.2.1.3.4 数据传输服务

（1）边缘集群数据传输要求

数据传输服务支持 Oracle 以及本次项目采购的 TP 数据库、AP 数据库、消息队列、内存数据库等数据源之间的实时同步和批量搬迁。主要用于计量自动化系统档案数据的实时流转和批量搬迁场景。

指标子项	具体要求
总体要求	提供了实时迁移、批量迁移、实时同步、数据订阅和实时灾备等多种功能。
功能要求	支持对数据迁移/同步的源端和目标端数据进行全量校验。
	支持数据同步任务监控报警功能。
	支持数据迁移/同步对库、表、列三级对象名映射。
	支持全量和增量迁移，增量迁移不影响源数据库业务。
	支持入云迁移和出云迁移两种模式。
	支持实例级、库级、表级迁移的对象选择；
	计量自动化系统 3.0 的数据库同步组件应支持主动访问源端数据库，

指标子项	具体要求
	实现实时数据同步。
数据加工	支持对同步的对象进行加工，即可以为选择的对象添加规则，在源库和目标库之间添加同步时间戳、添加附加列、列加工、字段选择、数据过滤。
容灾可用高	支持同城/跨城多机房部署，多机房高可用互备。 异常数据容错机制：支持将 record 同步报错的数据采集到一个异常版块，数据冲突记录
集群节点高可用	支持集群节点采用冗余架构，无单点故障，节点故障时任务的自动切换和恢复。 支持通过数据复制服务对云数据库实例进行跨区域的实例容灾复制。

（2）云边协同数据传输要求

根据云边协同技术规范，提供云边协同代理软件，实现采集监控域与数据分析域的云边协同能力，要求能支持数据分析域的数据库类型含大数据平台、关系型数据库等。

云边底座交互	根据云边协同技术规范，实现从生产控制云节点的云端管理中心获取标准底座部署文件、向云端管理中心上报边缘集群底座、组件和应用的部署信息，并根据实时性要求上报相关性信息。
云边制品交互	根据云边协同技术规范，实现与生产控制云节点的云端制品仓库对接，负责云边制品传递，结合主站业务应用的整体规划细化制品建设内容。
云边监控交互	根据云边协同技术规范，实现对边缘计算集群包括进程状态、告警信息、节点 CPU 利用率、物理内存利用率、虚拟内存使用率、磁盘使用率等状态的监控，并把底座、组件和应用的监控指标和告警信息，上报到生产控制云节点云端管理中心。
云边应用交互	根据云边协同技术规范，支持生产控制云节点部署的应用与边缘集群部署的应用进行双向交互，实现生产控制云节点和边缘集群应用的微服务相互调用。
	根据云边协同技术规范，支持云边库到库的数据实时增量同步，可以将边缘集群数据库等的档案变更数据可实时同步到云端数据库（实时增量同步）。
	根据云边协同技术规范，支持云边库到库的数据离线同步，可完成边缘集群数据库与云端数据库计算结果的双向数据同步（批量同步）。

（3）监控信息跨区域传输

分布式平台在安全III区可以获取各安全分区（Ⅰ区、Ⅱ区、接入区）的平台监控信息，并在安全III区集中展示。

7.2.1.3.5 数据库管理

数据库管理工具面向多种类型的数据库，提供集群管理、资源管理、配置管理、容灾备份、告警监控、日志管理等数据库管理功能。用户可以通过数据库管理工具界面操作创建数据库实例，用户授权，访问数据，管理数据。由于不同类型数据库的数据管理

操作存在差异，将按照 TP 库、AP 库和内存数据库三类描述数据库管理功能。具体要求如下表。

指标子项	具体要求
TP 数据库管理	支持历史执行 SQL 的模糊查询，可查看 SQL 执行的开始时间、数据库、SQL、状态、行数、耗时、备注等信息。
	支持图形化数据库备份恢复功能，工作备份恢复到新实例实现。支持表级别的备份恢复，可选是否对视图、存储过程、函数、触发器、事件等对象进行备份恢复。
	支持数据量统计，可以按照表名模糊查询，统计表行数、容量等信息。
	支持就地升级、灰度升级
	支持修改实例名称、重启实例、删除实例、节点替换、节点扩容等
AP 数据库管理	支持在管理界面中提供安装部署、集群管理、资源管理、配置管理、容灾备份、告警监控、日志管理、节点启停、补丁升级、节点替换等功能。
	支持对 AP 数据库所使用磁盘、网络、OS 的指标数据，关键性能指标数据进行收集、监控、分析。
	支持查看 AP 数据库各节点的可用状态、节点规格。
	支持在管理界面中创建、删除、更新数据库用户并进行权限管理。
	支持在管理界面中配置运维任务，创建运维计划并查看运维任务的运行结果。
内存数据库管理	支持在管理界面中创建、删除内存数据库实例，配置运行参数。
	支持在管理界面中变更内存数据库实例规格。支持内存数据库实例的扩容和缩容，实例变更规格后，不影响实例的连接地址、访问密码、数据配置等信息。
	支持在管理界面中完成内存数据库实例的主备切换。
	支持在管理界面中管理内存数据库的分片与副本、查看数据存储统计信息、查看慢查询日志。
	支持在管理界面中完成内存数据库实例诊断，通过实例诊断获取实例异常的原因、影响以及处理建议。
	支持在管理界面中完成内存数据库实例的备份和恢复。

7.2.1.3.6 数据库备份

数据库备份服务是为数据库提供连续数据保护、低成本的备份服务，它可以为多种环境的数据提供强有力的保护。数据库备份提供全量备份、增量备份和数据恢复能力。

指标子项	具体要求
功能要求	支持全量和增量备份保留时长配置到期自动删除。
	支持备份频率、周期、开始时间等备份计划配置。
	支持对主流数据库的备份与恢复。支持本次项目采购的 TP 库、AP 库的数据库备份。

指标子项	具体要求
外置存储池管理	支持备份到三方存储池，包括本地存储，对象存储
批量配置备份计划	支持相同的数据库类型和相同的备份类型的批量配置备份计划。
系统集成	数据库备份支持与云平台集成对接，实现单点登录、统一认证
集群高可用	数据库备份支持集群架构，避免因软硬件故障、误操作所造成的备份系统不可用。

7.2.1.3.7 数据库自治

数据库自治服务是一种对数据库进行运维，安全，管理的服务，有效保障数据库服务的稳定、安全及高效。

指标子项	具体要求
数据库自治AP 库功能要求	支持智能运维功能，为客户数据库的快速、稳定运行提供保驾护航的能力。对业务数据库所使用磁盘、网络、OS 指标数据，集群运行关键性能指标数据进行收集、监控、分析。通过综合收集到的多种类型指标，对数据库主机、实例、业务 SQL 进行诊断，及时暴露数据库中关键故障及性能问题，指导客户进行优化解决。
	支持 SQL 诊断和优化，定位 SQL 的性能问题，并输出 SQL 的优化建议。
	支持实时会话管理功能，提供实时活跃会话分析、实时会话数量、平均会话耗时、查询数量、平均查询耗时、平均查询等待时间等，支持快速定位活跃会话数量最多的用户、应用服务器。
	支持性能监控，提供集群、数据库和节点三种维度的监控视图，集群维度的监控指标：CPU 使用率，内存使用率，磁盘使用率，磁盘 I/O，网络 I/O，状态，CN 异常数量，只读，会话数量，查询数量，死锁数量，DN 异常数量，DN 实例 CPU 使用率，平均每秒事务数，平均每秒查询数。数据库维度的监控指标：查询等待队列长度，会话数量，查询数量，插入行数，更新行数，删除行数，容量。节点维度的监控指标：CPU 使用率、CPU 使用情况、内存使用率、内存使用情况、平均磁盘使用率、磁盘 I/O、TCP 协议栈重传率、网络 IO、磁盘容量、磁盘使用率、磁盘读速率、磁盘写速率、I/O 等待时间、I/O 服务时间、I/O 使用率、网卡状态、接收包数、发送包数、接收丢包数、接收速率、发送速率
	支持表诊断，通过收集数据表在关键运行状态的统计数据和诊断工具，快速地定位表的倾斜率和表的脏页率，以及对 DDL 进行规范性审核，方便用户对潜在的表定义问题提前感知。
	支持慢 SQL 分析功能，能够快速定位执行耗时 TOP 慢 SQL，通过定位 Top 耗时的查询，记录 Top SQL 耗时查询的变化历史记录。分析 Top SQL 查询出现的频率，定位慢查询。
	支持多维度的存储资源管理能力，包括 schema 维度空间管理，用于限制 schema 使用的永久空间大小和在用户维度的永久空间、临时空

	间和算子空间管理，防止单用户业务异常导致数据库只读。
	支持慢实例检测，可以通过周期性采集信息，将检测到的慢实例数据上报。用户可在界面上查看 24 小时内检测到的慢实例数量，以及在时间维度上的分布状态等信息，更为快捷地定位到拖慢整个集群的慢节点并分析其根因。
	支持负荷分析报告为数据库提供性能数据收集和分析，用户可通过创建负荷信息快照记录指定时间段集群的负荷信息数据。其中两个负荷信息快照可形成该时间段内负荷诊断报告。负荷诊断报告可以提供指定时间段内的性能数据，以报告的形式呈现给用户，能够帮助用户发现异常、诊断问题、优化性能等，为数据库调优提供输入。
数据库自治 TP 库 功能要求	慢 SQL 诊断帮助开发者回溯执行时间超过阈值的 SQL，诊断 SQL 性能瓶颈。通过自定义采集方案，帮助用户快速锁定关键慢 SQL，并在慢 SQL 文本、执行计划和其他信息的基础上，基于特定规则对慢 SQL 进行根因分析，给出慢 SQL 优化建议，效率提升百倍。
	索引查询帮助识别冗余/无用索引，推荐好的索引，优化数据库查询速度。支持原生的索引推荐功能，通过系统函数及运行工具等形式进行单条索引推荐及负载级别索引推荐，大幅度减少磁盘扫描的次数，提高负载执行效率。
	趋势预测对增长型的容量指标做趋势预测结果和风险提示，降低数据库异常风险。通过监控数据库指标，并基于时序预测和异常检测等算法，发现异常信息，进而提醒用户采取措施，避免异常情况造成严重后果。
	会话查杀帮助定期检查和终止会话，以释放资源，提高数据库性能和增强系统安全性。通过安全筛选机制，保证用户使用会话查杀时可以专注于自身业务的会话，而不会误操作系统级别会话从而影响系统的正常运作。
	全量 SQL 可以有效地帮助业务进行数据库审计，快速排查性能问题。通过内存式记录、采集以及流式转储方案，将全量 SQL 对数据库的性能损耗降到最低。
	为避免服务器过度负荷，提高系统可靠性、稳定性，可以在必要时执行限流措施，提高系统性能。
	支持将单次业务计划调优的任务量从业务升级降级为单条运维语句。避免直接修改业务语句，通过调用数据库提供的接口，对指定的查询语句模板进行 hint 调优。
	执行计划绑定可以讲查询和优秀的执行计划进行绑定，避免不同执行计划造成业务性能抖动。通过 SQL 的计划管理功能，给指定 SQLID 绑定执行计划，解决执行计划跳变问题，也可以通过绑定更优的执行计划获得更好性能。实现了以通用计划为基础的计划二级缓存机制实现计划快速替换。
	巡检对系统资源状态，数据库实例基本信息、健康状况、异常告警、性能指标等统计分析，并对其中关键资源指标趋势进行风险判断，避免潜在不易发现的问题影响实例健康。提供日常巡检功能，支持自定义巡检项，相比友商有更丰富的周期设置，及时发现问题，提高系统稳定性和效率。

7.2.1.4 中间件服务

7.2.1.4.1 企业级分布式应用服务（微服务）

企业级分布式应用服务是一个应用托管和微服务管理的云原生 PaaS 平台，提供应用开发、部署、监控、运维等全栈式解决方案。企业级分布式应用服务是分布式架构和数字化业务上云的应用托管平台，具有广泛的应用场景。

指标子项	具体要求
应用生命周期管理	提供 WEB 界面形式的可视化分布式应用管控平台，对应用进行生命周期管理，包括而不限于应用的创建、部署、启动、扩容、停止和下线。
框架兼容性	支持原生 SpringCloud、Apache Dubbo 微服务应用托管与治理，存量应用零修改，可无缝迁移。
	微服务应用与运行环境不绑定，支持原生版 tomcat/SpringBoot
应用支持	支持集成安全自主可控应用服务器
弹性伸缩	支持应用实例通过手工或自动弹性伸缩
环境管理	支持多种类型环境管理（开发、测试、预发、生产环境），支持纳管基础资源（计算、存储、网络、数据库等）。应用与资源视图分离，从应用角度，可以部署到不同环境。
服务鉴权	在分布式服务框架控制台上可以创建和管理服务鉴权规则。根据鉴权规则，被调用方将可开闭允许或禁止调用方调用其接口，进行服务调用的安全管控。
应用托管	支持多种部署格式，包括：jar、war、容器镜像、源代码包，降低部署难度，提升效率。
灰度发布	以灰度方式发布应用。发布过程支持分批操作以保证业务连续性。支持按内容和按比例的灰度发布策略。发布应用的过程中支持配置启动命令、环境变量和应用生命周期管理。
微服务注册发现	支持服务自动注册与发现，无需配置地址即可实现分布式环境下的负载均衡，并支持多种路由策略及健康检查。提供手动上下线微服务功能。
动态配置	提供应用运行时动态修改配置的服务，并提供图形化的集中化管理界面。支持配置动态推送实时生效，支持配置灰度：按应用、微服务级别推送配置，支持将应用、微服务打标签，按标签自定义推送范围
微服务治理	支持按照权重、轮询、随机等负载策略，支持可用区就近路由，支持按微服务版本号切分流量，支持按请求参数切分流量，参数来源可以是 HTTP Header、Query Param 等。支持微服务仪表盘，显示微服务实时吞吐量、平均时延、请求失败率、请求数、熔断数、请求超时数、熔断状态等等
安全合规	支持管理面容灾，注册中心、配置中心支持双活部署，支持国密算法。

7.2.1.4.2 消息队列

消息队列基于高可用分布式集群技术，提供消息订阅和发布、消息轨迹查询、定时（延时）消息、资源统计等一系列消息云服务，是企业级外网（综合数据网等）架构的核心产品。为分布式应用系统提供异步解耦、削峰填谷的能力，同时具备海量消息堆积、高吞吐、可靠重试等外网（综合数据网等）应用所需的特性。支持 HTTP Restful API 和 TCP 协议，支持 java、python 等多语言 SDK，方便不同编程语言开发的快速接入消息云服务。核心能力需要支持如下：

指标子项	具体要求
实例管理	支持服务实例查询、创建、修改、删除等操作。服务实例列表展示了用户创建的所有服务实例，服务实例详情展示了服务实例的基础信息，包括实例连接地址、组网等信息。
分布式消息部署	支持主备模式多节点集群模式，跨数据中心的多集群模式，跨数据中心的消息平台通过统一路由连接。
定时消息	支持消息查询，通过指定时间和位置，查询具体消息的内容。
分布式事务消息	提供分布式事务消息功能，保证发送消息与用户业务逻辑之间的一致性，当用户业务执行成功时，消息才被提交，否则消息被回滚。
定时消息	支持消息查询，通过指定时间和位置，查询具体消息的内容。
实例间消息同步	支持消息路由，通过级联的方式，实现实例或节点之间数据复制及同步。
支持 TCP、HTTP 协议接入	支持消息队列多协议接入，支持 HTTP Restful API 和 TCP 协议，提供管理控制台及管理 API，支持 TCP 协议 SDK，支持 HTTP 协议 SDK 接入。
死信队列	支持查询无法被正常消费的消息并可以进行重投。
消息回溯	支持对已消费过的消息重新消费。
消息查询	支持按照 Topic、消息 ID、应用 ID、消息分区、生产日期等多维度的条件查询。
消息监控	支持按分区数监控、主题数监控和消息堆积数监控等。
消息轨迹	支持消息轨迹查询，查看消息生产与消费的轨迹，包括客户端 IP 查看、生产时间查看、消费时间查看、消息同步时间查看等功能。
顺序消息	按照消息的发布顺序进行顺序消费，支持全局顺序与分区顺序。
运维能力	支持简单便捷的消息重置、消费组管理等，支持界面对于消费组详情进行查询和管理，提升租户侧消息自运维能力。提供实例诊断能力，方便用户诊断实例消费组积压情况，一键诊断、快速定位
认证和访问控制	支持客户端连接进行访问认证和 topic 权限管控，提供 APP 认证能力以及 Topic 订阅和发布等权限授权能力
消息数据高可靠	支持消息持久化，多副本存储机制。可选择副本间消息同步、异步复制，数据同步或异步落盘等多种方式。
容灾高可用	在 Region 仅具备 2AZ 条件环境下，支持客户发放跨 AZ 高可用实例，并且保证业务的高可用切换
应用隔离	基于应用的权限，控制 Topic 消息的收发权限。

指标子项	具体要求
多语言支持	支持 java、C/C++、.NET 等多语言 SDK。

7.2.1.4.3 应用实时监控

应用实时监控服务是一款云应用性能管理类监控产品。可以基于应用和业务自定义等维度，迅速便捷地为企业构建秒级响应的业务监控能力。

指标子项	具体要求
应用节点监控	提供对于应用部署集群及单节点的 CPU，内存，磁盘、网络的监控并以图形化形式按照小时，天，周进行曲线展现。
监控应用框架支持	支持基于主流同步、异步调用框架，如 Dubbo, gRPC，HTTP RESTful 的分布式链路跟踪。
全息排查	支持全息排查，将调用链路信息与业务事件进行集成，将业务事件通过调用链的 traceID 进行双向关联，当业务出现异常时可以基于业务事件关联的链路追踪信息进行问题排查
定时任务监控	提供定时任务的详细监控，包括概览、SQL 调用分析、NoSQL 调用分析、异常分析、错误分析、链路下游和调用链查询。
池化监控	提供 tomcat 容器所使用的线程池的各项指标，包括当前线程数、最大线程数、活跃线程数和队列大小。线程池类型至少包含：Tomcat
线程栈分析	提供线程粒度的 CPU 耗时和每类线程数量的统计，可以根据 CPU 耗时统计快速发现异常线程。针对异常线程支持 CPU 耗时和线程数曲线图分析 CPU 耗时与线程数变化，支持查看线程的方法栈的关键信息，查看指定时间内的真实运行线程信息
JVM 监控	支持应用层监控，包括但不限于 JVM 的 YoungGc 及 FullGc 的数量及耗时、JVM 的堆内存使用情况、JVM 的堆外内存使用情况、JVM 线程数等维度的监控。
依赖拓扑图	能统计出服务和服务的关联依赖图
外部调用监控	可以查看该应用的所有外部调用的请求数、响应时间、错误数及 HTTP 状态码信息
应用接口监控	支持应用接口的指标统计，包括请求数，响应时间和错误数等
应用标签能力	支持对应用进行标签分组与过滤
应用监控报警能力	支持默认提供应用各维度指标的报警，包括但不限于 JVM、异常接口调用、应用调用类型统计、主机监控、数据库指标等应用监控的风险信息进行报警
应用监控自定义设置	支持自定义应用监控的一些常用设置，包括但不限于 Agent 开关、慢请求阈值等。
异常分析	支持统计指定时间范围的异常次数，以及异常的详细信息包括异常接口名称、异常信息摘要、占比、异常堆栈，以及触发该异常的调用链路
接口快照	提供接口快照功能，接口快照支持通过自动线程剖析定位慢调用方法
数据库调用	支持抓取 sql 语句运行时长和错误，统计数据库慢查询的请求次数及

指标子项	具体要求
监控	耗时，对数据库的性能问题有针对性监控
服务 MQ 调用监控	支持服务 MQ 调用信息查看，支持按消息 topic 维度展示请求数，响应时间和错误数
用户自建应用监控	支持用户自建应用监控
自定义监控报警能力	支持基于用户自定义监控数据集指标的报警
调用链多条件查询	通过 TraceId 精确查询调用链路详细情况，或结合多种条件筛选查询调用链路。
链路跟踪	支持 Web 界面可视化的调用链路的跟踪展示
NOSQL 调用统计	支持指定时间段内 NoSQL 调用次数统计，支持基于操作命令的调用平均耗时、调用次数的详情查看。NoSQL 类型至少包含 Redis，MongoDB、ElasticSearch
编程语言支持	针对 Java 语言应用，支持通过探针方式提供应用监控，为 Java 应用安装 Agent 后，即可开始监控 Java 应用，无需代码侵入。 针对其他语言提供 OpenTelemetry、Zipkin、Jaeger 中至少一种客户端接入方式。 。
易用性	指标数据支持基于数据集配置交互式大盘，大盘可动态刷新。

7.2.1.4.4 云服务总线

云服务总线具有服务协议适配和开放管控能力，可以实现跨环境、跨协议的服务互通，主要针对应用系统能力对外开放和服务互相访问的场景，提供统一的安全授权、流量限制等管理和控制。

云服务总线具有协议适配能力，支持常用协议服务的接入和开放，支持多种服务注册发现机制，微服务以及遗留系统的服务可以直接在云服务总线上开放成 API，云服务总线还支持跨环境联动，允许像访问本地服务一样访问其他环境的服务。

指标子项	具体要求
API 生命周期管理	支持从 API 设计、发布、授权、测试和监控等全生命周期管理。
API 级联发布	支持同一区域或不同区域的两个实例可以建立级联关系，级联实例中的 API 可以使用被级联实例中的 API 作为后端服务，实现跨实例间的 API 调用。级联实例间的 API 调用使用专属的认证通道。
API 调试	支持 API 的在线调试能力。
API 编排	支持通过定制 js 脚本，完成服务的编排封装。
协议转换	支持 API 协议&数据格式转换， Rest 转 soap， Json 转 Xml 等
策略路由	提供 API 策略路由能力，支持根据不同的 Header、Query 来定制 API 接口的后端。
实例扩容	支持规格或版本间升级扩容，以满足集成业务量增加和集成架构的持

指标子项	具体要求
	续演进；
流量控制	支持秒级 API 流控，针对不同的业务等级、用户等级，可实施 API 级别的精细流控，保护集成业务的稳定运行
监控管理	支持 API 的监控统计和分析
黑白名单管理	可设置服务黑白名单，无需重启服务即可生效。
安全认证	支持 app key&app Secret 对应用进行认证，用户可编写自定义脚本对接第三方认证。支持 SSL 证书加密。
云边应用交互	支持对接微服务引擎，统一治理系统入口流量和微服务流量。

7.2.1.4.5 日志服务

日志服务是针对日志类数据的一站式服务，能快捷完成日志数据采集、消费以及查询分析等功能，提升运维、运营效率，建立海量日志处理能力。

日志服务具有如下功能：日志采集、查询分析、告警、实时消费等。

日志服务的典型应用场景，包括数据采集、实时计算、数仓与离线分析、产品运营与分析、运维与管理。

指标子项	具体要求
总体要求	针对实时日志类数据一站式服务，无需开发就能快捷完成日志数据采集、消费、投递以及实时查询分析等功能，提升运维、运营效率，建立海量日志处理能力
功能要求	支持 json、文本、数值等数值类型查询、支持 json 格式中文本自动构建索引、支持对数据进行全文查询、支持多个条件组合查询（And、Or、Not）、支持原始日志中上下文查询（前后 N 行）
	日志采集工具支持使用分隔符、正则表达式对文本文件内的日志采集、支持 syslog 协议、Kubernetes 日志采集
	原生支持数据投递功能，可将采集到的日志通过控制台进行投递，便于长期存储数据或联合其他系统消费数据。
	支持数据多重冗余备份，最大支持 3 个节点故障而业务数据不丢失
	支持时序数据采集存储，数据包含主机监控、Telegraf 数据、Prometheus 监控数据，可以支持 SDK 采集数据。
安全性	日志服务通过对数据进行加密存储，提供数据静态保护能力。
性能指标	支持千亿日志查询的秒级返回

7.2.1.4.6 API 网关

API 网关提供完整的 API 托管服务，覆盖 API 全生命周期管理，包括 API 设计、开发、测试、发布、运维监测、安全管控、下线等 API 各个生命周期阶段、运维监测、安全管控等 API 各个生命周期阶段。快速构建以 API 为核心的系统架构，满足新技术引入、

系统集成、业务中台等诸多场景需要。提供防攻击、防重放、请求加密、身份认证、权限管理、流量控制等多重手段保证 API 安全，降低 API 开放风险。

指标子项	具体要求
统一接入	支持从 API 设计、发布、授权、测试和监控等全生命周期管理，同时提供密钥管理、访问控制等功能，并提供外部接口允许第三方系统接入；
协议支持	支持 HTTP、HTTPS 协议、websocket 等
服务编排	支持服务的编排封装，并开放成新的 REST API。
安全管控	支持多种安全认证方式，包括 app key&app Secret 对应用进行认证，用户可编写自定义脚本对接第三方认证。
	支持多种访问控制方式，包括 IP 访问控制、账号名、账号 ID 访问控制。
	支持秒级 API 流控，针对不同的业务等级、用户等级，可实施 API 级别的精细流控，保护集成业务的稳定运行
请求转发	支持参数映射，可以从请求的 Query 和 Header 读取参数，并映射到后端
API 接口	支持 API 策略路由能力，支持根据不同的 Header、Query 来定制 API 接口的后端。
运维监控	发布管理。支持在不同环境中发布和下线，可以通过不同 header 方式访问到不同环境的 API，支持已发布的 API 快速切换到不同的历史版本。
	支持 API 的监控统计、日志分析、监控展示；支持 API 访问日志输出。
集成能力	支持数据库到 API 的转换发布能力，降低应用开发的用数难度，支撑应用快速创新，支持 SQL 转换为 RESTful 等 API 接口

7.2.1.5 数据计算组件

7.2.1.5.1 实时计算

实时计算是一种持续、低时延、事件触发的计算任务，实时计算可以有效地缩短全链路数据流的时延、实时化计算业务逻辑和平摊计算成本，最终有效满足实时处理大数据的业务需求。典型适用场景：实时 ETL&索引构建、实时统计&分析、监控预警等。

指标子项	具体要求
实时数据采集	提供实时数据采集工具，支持增量数据集成（CDC），支持关系型数据库 binlog 到数据计算组件的实时增量同步。
	实时数据采集工具支持按照表进行并发采集，支持单任务多表并发，支持分布式部署和线性扩展。
	实时数据采集工具源端应支持 Oracle 及国产主流数据库等数据源。
实时流处理	提供实时流处理组件。

指标子项	具体要求
	支持流批一体，可以在同一套开发平台中定义批量计算作业和流式计算作业。
	支持在流上执行类 SQL 任务，SQL 能力至少包括：过滤、转换、基于窗口的计算能力、提供窗口数据的统计能力、关联能力、流数据的拆分与合并。
	支持可视化 Flink SQL 作业提交和任务管理能力。

7.2.1.5.2 数据离线计算

数据离线计算提供基本的分布式存储能力，支持 PB 级别数据处理与计算，支持结构化与非结构化数据存储、支持列式存储、提供完善的多备份机制、支持文件的高并发、大吞吐的读写操作。主要应用于日志分析、机器学习、数据仓库、数据挖掘、商业智能等领域。

指标子项	具体要求
集群规模	超大规模节点调度能力，具备万级节点调度能力。为保证大数据集群具有高可扩展性。需提供第三方测评报告
功能特性	支持 MapReduce 类型的分布式计算任务，支持 DAG 模式的作业处理方式。
	支持 Apache Spark 编程接口，用户可以使用 Spark 接口进行编程处理存储在大数据计算服务中的数据。
	支持多种计算框架如 SQL，MapReduce，Spark，Flink。
	提供离线数仓组件（如 Hive）。
	提供全文检索组件（如 ElasticSearch）。
	离线计算数据存储采用列式存储方式。
	分布式文件系统支持小文件合并。为避免小文件过多导致分布式文件系统作业性能降低，数据计算组件应提供小文件合并能力，支持扫描表中低于设定阈值的小文件，支持根据用户设置的合并后的平均文件大小进行文件自动合并，加速分布式文件系统海量小文件场景下的数据检索能力。
	数据计算组件支持滚动升级能力，组件升级时业务不中断。支持一次升级少量节点、循环滚动，直至集群所有节点完成升级。
	支持自动健康检查与巡检，可实现健康度巡检和审计，保障系统的正常运行，提升运维效率。
湖仓一体	支持构建实时数据湖。数据计算组件在分布式文件系统之上，支持对数据做更新删除和增量数据处理，可提供与 Delta lake、Iceberg、Hudi 等类似的增量数据处理方案。
跨源计算	支持跨数据源的协同计算和协同查询能力。支持数据源包括：离线数仓、分布式列存数据库、全文检索组件、AP 库等。提供物化视图 SQL 语法，支持物化视图的自动刷新。
备份策略	支持对数据计算组件的组件元数据或者组件业务数据，做全量和增量

指标子项	具体要求
	备份，并支持将已备份的数据恢复到集群中。

7.2.1.5.3 分布式消息队列

分布式消息队列是流式数据的处理平台，提供对流式数据的发布、订阅及分发功能，让用户可以轻松构建基于流式数据的分析和应用。

分布式消息队列服务可以对各种移动设备、应用软件、网站服务、传感器等产生的大量流式数据进行持续不断的采集、存储和处理。用户可以编写应用程序或者使用流计算引擎来处理写入到分布式消息队列的流式数据。

分布式消息队列具有高可用、低延迟、高可扩展、高吞吐的特点。分布式消息队列与实时计算引擎无缝连接，用户可以轻松使用 SQL 进行流数据分析。分布式消息队列服务也提供分发流式数据到各种云产品的功能。

指标子项	具体要求
功能特性	提供分布式的消息发布-订阅系统，支持 Kafka 组件或兼容 Kafka 发布-订阅接口的其他组件。
	支持消息持久化、高吞吐、分布式、实时、多客户端支持等特性。
	支持 Web 管理界面，可通过 Web 界面完成集群状态检查、管理主题、管理分区等操作。
	支持用户粒度连接数控制
	支持告警监控和健康检查。
可靠性	支持 At-Least Once， At-Most Once， Exactly Once 消息可靠传递。
	支持分布式消息队列的元数据备份与恢复。
多协议支持	支持通过多种协议生产消费数据，包括：SASL_PLANTEXT 协议、SASL_SSL 协议、PLANTEXT 协议、SSL 协议等。

7.2.1.5.4 数据开发组件

数据开发组件，能帮助快速完成数据同步、开发、治理、服务、质量、安全等全套数据研发治理工作。具备海量数据的离线加工分析、数据挖掘的能力，也集成了数据集成、数据开发、生产运维、实时分析、资产管理、数据质量、数据安全、数据共享等核心数据工艺，同时还提供了数据服务，让数据从采集到展现、从分析到驱动应用得以一站式解决。

指标子项	具体要求
数据同步	支持在本项目范围内的关系型数据库、AP 库、离线数仓、分布式列存库等多种同构、异构数据源之间的双向数据同步。
	提供可视化的连接和任务创建、编辑界面，用户通过菜单配置方式完

指标子项	具体要求
	成数据源连接和数据同步任务创建和管理。
	支持多种数据同步场景，包括：计量自动化系统分布式平台内部的数据双向同步，计量自动化系统分布式平台内部与外部数据源的数据双向同步。
数据开发	支持通过图形化所见即所得的 ETL 编辑器实现 ETL 能力，支持数据抽取、清洗、转换、加载，用户可以避免写大部分 SQL、Python、Java 代码。
	支持 SQL 脚本编辑器，编写 SQL 代码的过程中支持代码格式化、代码补齐、关键词高亮等编辑器常用操作。
	支持多种大数据服务引擎编排，包括数据计算组件（如 Hadoop）、AP 库、离线数仓等。
	提供作业运维功能，支持重新执行某批次任务，给作业补充数据，对运行中作业暂停部分节点。
	提供作业调度功能，支持时间周期调度，支持事件驱动调度，支持设置作业间的依赖关系。
	支持作业链路监控，实时显示作业上各节点的执行状况。
	数据开发支持开发环境与生产环境隔离，任务开发调测完成后通过提交与审批后可发布到生产环境。
数据治理	支持自定义数据标准模板，支持自定义表模型的基础属性与列属性。
	支持模型管理、逆向数据库、主外键管理、分区设计，可以管理物理模型和逻辑模型，支持逆向数据库等功能。
	维度建模，支持基于事实表的星型模型与雪花模型建设，支持多级维表管理。
数据质量	支持自动化生成数据质量审核任务。
	支持质量统计功能，展现质量报警和质量规则统计信息。
	支持规则管理功能，支持基本数据质量监控规则。
	支持生成数据质量报告。
	支持质量规则通过数据开发功能进行关联调度，自动生成质量监控结果。
数据资产	支持多种数据连接，包括 TP 数据库、AP 数据库、大数据等数据源连接。
	支持生成数据资产报告，包括各资产目录下的表分布、表容量、表行数、资产的数据密级等。
	数据资产支持准实时元数据采集。支持准实时分钟级同步元数据变化，并准实时采集更新元数据信息。
	支持数据源元数据采集和存储；支持配置采集策略，选择需要采集的数据库、数据表、时间范围；支持采集任务调度策略，支持周、天、小时、分钟定时调度或手动调度等。
	支持数据资产概览。可以从数据表大小、来源、数量和热度等维度统计数据资产情况。
	支持数据表血缘关系查看，包括血缘和影响，支持数据处理全过程血缘。
	支持标签定义和管理。支持给数据资产打标签。

指标子项	具体要求
数据服务	支持在线开发、调试、发布数据服务 API，通过配置、脚本实现在线零编码开发和在线调试。
	支持关系结构化数据源和非结构化数据源。
	支持自定义 API 流控策略，可从时长、API 流量限制次数、用户流量限制等方面进行流控策略设置。
	支持数据服务发布，数据服务开发者可以选择是否将数据服务 API 发布。对于发布之后的数据服务 API，消费者可以去查看服务的详情并申请使用。
	支持给数据服务开发者和数据服务消费者提供 API 监控信息展示。
数据安全	支持通过创建权限策略实现对数据资源的访问控制。
	支持对数据资源权限的申请与审批。
	支持通过用户创建或内置的数据识别规则自动发现敏感数据并进行分级分类，支持手动修正不准确数据。
	支持通过数据脱敏、数据水印等方式实现敏感数据保护。
	支持进行数据 ETL 流程图设计，支持 join 关联可视化、join 关联手动编辑、join 关联字段的自动识别主外键等。 支持数据的清洗功能，包括数据补空、去重重复数据、去除空格、缺失值填充、筛选过滤、格式转换、分组汇总、自循环列、数据列自定义拆分、镜像（数据处理的结果集复用）、排序、抽样、范围分组和新增自定义数据字段等。
	支持数据源血缘分析，展示报告所依赖的数据源、数据集、数据库及数据库表

7.2.1.5.5 数据管理组件

数据管理组件支持从业务、服务、集群和主机等多个角度对大数据产品进行运维。除此以外，还需支持对大数据产品进行补丁升级、自定义大数据产品的报警上报配置、查看数据管理组件的运维操作历史等。通过数据管理组件，平台运维人员可以管理大数据产品，例如：查看大数据产品的运行指标、修改大数据产品运行配置、查看并处理大数据产品的报警等。

指标子项	具体要求
监控运维	提供统一的仪表盘，包括流量、延时、资源使用率等核心指标
	提供统一的管理界面，可以在一个管理界面中完成：软件安装、补丁应用、配置管理、备份与恢复、集群节点启停、服务启停、服务部署、租户管理、资源分配等操作。
	支持自动健康检查与巡检，支持系统运行健康度巡检和审计。
	支持动态扩缩容数据计算组件的集群，支持集群大规模滚动升级，升级过程中平台组件正常提供服务。
运营分析	支持多个统计纬度的大数据集群资源分析视图，支持租户资源的动态配置和管理，资源隔离，资源使用统计等功能。

指标子项	具体要求
	提供图形化的集群健康检查工具，能够检查集群相关节点、服务的健康状态，发现数据计算组件的潜在风险，并生成健康检查报告。

7.2.1.6 能力开放中心

7.2.1.6.1 协同研发平台

基于 DevOps 理念搭建，重视软件开发人员（Dev）和 IT 运维技术人员（Ops）之间沟通合作的文化和惯例，为企业提供包含流水线管理、代码管理、制品管理等在内的开箱即用一站式服务。提供开放式的 DevOps 工具链选型，在平台中深度集成敏捷项目管理、代码管理、CI/CD、制品管理、制品质量分析等类别中的主流工具并灵活兼容客户已有的工具选型，灵活实践 DevOps。

指标子项	具体要求
图形化编排流水线	支持用户使用图形化界面编排流水线，包括更新、复制、删除、取消和查看、删除执行记录
模板创建流水线	支持用户使用流水线模板创建流水线
多分支流水线	用户创建和使用多分支流水线等功能，简化容器应用自动化发布的流水线的创建和使用难度，提升应用的发布效率。
代码提交触发流水线执行	支持代码仓库中代码提交时自动触发流水线执行
Tag 创建触发流水线执行	支持代码仓库中 tag 创建时自动触发流水线执行
PR 创建触发流水线执行	支持代码仓库中 PR 创建时自动触发流水线执行
自定义时间触发流水线执行	支持设置自定义时间自动触发流水线执行
新增镜像触发流水线执行	支持被监听的镜像品库新增镜像时会触发流水线执行
新增制品触发流水线执行	支持被监听的制品库新增制品时会触发流水线执行，提升应用各个阶段的自动化发布能力。
流水线通知	支持将流水线执行结果发送给用户，第一时间能够发现应用的发布状态，并根据通知进行调整和查看。
集成项目管理工具	支持集成项目管理工具
集成 CI 工具	支持集成多种持续集成工具
集成代码仓库	支持集成代码仓库，实现代码管理；
集成代码扫描工具	支持集成代码扫描工具，实现代码质量分析
集成制品仓库	支持集成多种制品仓库，实现制品管理，并可以通过集成已有敏捷工具提供扩展工具支撑能力

7.2.1.6.2 BI 报表工具

BI 报表工具可以提供海量数据实时在线分析服务。通过提供智能化的数据建模工具，极大降低了数据的获取成本和使用门槛；通过拖拽式的操作和丰富的可视化图表控件，轻松自如地完成数据透视分析、自助取数、业务数据探查、报表制作和搭建数据门户等工作。

指标子项	具体要求
可视化分析	支持丰富的图表。支持柱图（2D/3D）、堆积柱图（2D/3D）、饼图（2D/3D）、线图、平滑线图、环形图、面积图、雷达图、瀑布图、气泡图、散点图、词云、仪表盘、矩阵树图、象限图、直方图、漏斗图、桑基图、关系图、旭日图、富文本（支持参数）等多种展现形式。
	支持下钻、联动、跳转、辅助线、趋势线、预测线
	支持将仪表板拖拽式组装为数据门户，支持内嵌链接， 支持模板和菜单栏的基础设置。数据门户不仅可以引用数据分析软件中的数据结果，同时也支持外挂链接。支持电子表格，兼容 excel 或数据库 sql 函数。 支持图表排序（降序、升序、手动排序、聚合排序）
数据预处理	支持直接跨库、跨数据源关联数据 支持通过可视化的拖拽操作进行数据建模和表的关联
填报及流程审批	支持自定义设计填报页面，支持可视化方式的数据填报，支持增量和全量数据填报，支持流程审批
数据建模	支持各类自定义 SQL 功能。数据建模负责数据源的 OLAP 建模过程，将数据源转化为多维分析模型，支持维度（包括 日期型维度、地理位置型维度）、度量、星型拓扑模型等标准语义，并支持计算字段功能，允许用户使用当前数据源的 SQL 语法对维度和度量进行二次加工
数据接入	支持国产主流数据库及本项目提供的所有数据库类型。
分析工具	支持帕勒托分析（Pareto Analysis）：又称为 80/20 法则，这是一种决策工具，用于识别和优先处理问题或任务中最重要的因素。帕勒托原则认为，在许多情况下，大约 80%的效果来自 20%的原因。在实际应用中，这可以帮助管理者集中资源和努力在产生最大影响的关键因素上。
	支持正态分析（Normal Analysis）：正态分析通常指的是对数据集进行正态分布的检验。正态分布是一种在自然和社会科学中非常常见的统计分布，其特点是数据呈对称的钟形曲线分布。通过正态分析，可以判断数据是否符合正态分布，这对于许多统计测试和概率计算至关重要。
	支持四象限分析（Quadrant Analysis）：这是一种将数据或项目根据两个维度（通常是重要性和紧急性）分类的方法。最著名的例子是艾森豪威尔矩阵（Eisenhower Matrix），它将任务分为四个象限：重要且紧急、重要但不紧急、不重要但紧急、不重要且不紧急。这种方法有助于个人和团队更有效地管理时间和优先级。
	支持五 W-H 分析（5W1H Analysis）：又称为六何分析，是一种问题解决和决策制定的工具。它包括以下六个问题：What（什么）、Why（为什么）、Who（谁）、Where（哪里）、When（何时）和 How（如何）。

指标子项	具体要求
	通过回答这些问题，可以帮助人们全面理解情况，识别问题的根本原因，并制定有效的解决方案。

7.2.1.6.3 数据可视化

数据可视化是集数据接入与处理、数据分析、数据展示和数据业务协同为一体的数据可视化分析平台，能够快速完成数据接入与处理、可视化页面设计、数据分析、业务协同应用与分析支持等功能，帮助管理者洞察数据、发现和应用数据的价值，为直观、科学的业务分析提供支撑。

指标子项	具体要求
数据源支持类型	支持标准的 JDBC 接口，能直接对接各种主流关系型数据库系统，包括国产主流数据库，以及本项目所提供的所有数据库。 支持文本数据（Excel、CSV、TXT）的直接导入分析，支持对文件数据源进行追加导入，支持修改入库时的字段名和类型。 支持空间数据源的接入，以及直接连接标准服务等空间数据服务。
流程式数据集建模	提供图形化流程式的数据集建模能力，支持一个或者多个数据节点、数据预处理节点按照业务需要的方式串行组合起来建模。数据预处理节点包括：联接、合并、筛选、计算字段、清洗节点、列转行、行转列、拆分列、分组汇总等。 数据集构建过程中支持从数据源中拖出多张表，然后设置他们的关联关系，即可形成一个物理数据模型（数据节点）。表关联时支持左联、右联、全联等，直接选择配置。同时支持通过手动编写 SQL 语句的方式构建物理数据模型，实现表关联、表合并需求。 构建好的数据集提供数据类型转换、字段名称修改、字段隐藏等功能，支持数据的实时预览。
跨源数据处理	在构建数据集时，支持选择多个数据源（可以是不同的数据库之间、数据库与文本数据源等）中的表或者字段进行关联、合并、计算等处理。
数据指标构建	提供指标管理模块，支持构建指标分类和指标，每个指标分类包含多个指标。一个数据指标是包含多个维度（修饰词）和一个度量，并具备一定计算规则的结果性业务数据描述，是在数据集的基础上再次对数据进行业务化抽象。支持基础指标与复合指标的定义，复合指标是通过对单个或者多个指标定义业务运算而创建。可通过 Excel 方式导入导出整个指标体系或单个业务专题指标，以实现指标体系的备份或者迁移。
组件样式设置	图表组件平均提供 100 多项不同的参数设置，细化到图表的色系、标签、提示框、图例、坐标轴、鼠标交互样式、组件动效等属性配置，组件配置的样式、效果和数据所见即所得。
属性样式批量设置、样式格式刷	支持对选中的多个同类型组件的属性样式进行批量设置，也支持对不同类型组件的公共属性样式进行批量设置。

指标子项	具体要求
条件渲染与动态告警	支持对图表类组件进行条件渲染设置，当组件所涉及的数据满足配置的条件，则根据配置渲染出不同的样式，让相关数值高亮呈现。同时，支持设置动态告警预警分析计算，包含：告警条件、告警等级、红灯提醒样式。在页面不刷新时，平台也能定期对告警条件进行计算。如果数据达到条件，则相应图表进行红灯提醒和样式渲染。
可视化卡片设计	支持将一个或者多个组件组合为一个具有一定业务意义的可视化卡片。可视化卡片中包含了样式、数据以及内部的业务逻辑配置，可独立地运行和查看。 提供专门的卡片管理，能新建、发布、授权、复制、删除、导入、导出、调整分类等。也支持在页面设计器中选择多个组件快速保存为一个可视化卡片。
事件动作执行	支持事件动作类型包含：联动、打开链接等。联动：即支持页面内、页面之间的组件联动。联动组件时支持多种组件响应动作，包括但不限于：刷新数据、组件显示、组件隐藏、动态模型绑定、切换组件显示隐藏、设置组件值等。不同的被联动组件具有不同的组件响应动作。支持联动多个组件。打开链接：支持打开当前工程页面、跨工程页面以及手动输入外部链接等，还支持跳转到页面参数、组件属性参数中的链接地址。链接打开的方式支持新建浏览器页签、新建浏览器窗口、当前页面打开、从内部框架打开。打开链接时还支持为这些链接传递一个或者多个参数。调用服务：支持通过 GET/POST 方式调用外部服务。
事件相关参数	在人机交互配置过程中，各个环节在使用参数时，都支持选择页面参数、系统变量、组件属性参数、事件触发参数。系统变量可包含：本地时间、服务器时间、用户 ID、用户名、部门名、部门 ID。组件属性：各个组件开放出来的可获取的属性、数据值，比如，当前选中值、当前文本值、开关状态等。
底图服务接入	提供底图服务接入能力，支持 WMS、WMTS 及 XYZ 类型的底图服务接入。
GIS 可视化场景编辑	支持独立的自助式二维、三维 GIS 可视化场景编辑器，分别支持平面地图和球面地图。 全图形化配置界面，包含：底图选择区、图层管理区、图层参数配置区、场景配置区、效果预览区等。 底图选择区：支持选择单个服务作为底图，也可选择多个底图进行叠加，形成一个底图； 图层管理区：支持自定义添加分组，提供对图层的统一管理功能，包括但不限于：图层拖动排序、图层显示/隐藏、图层复制、图层删除等； 图层参数配置区：每个图层提供多个参数配置，包括图层的基础信息、样式配置、标注配置、信息窗配置、条件渲染配置等； 场景配置区：提供针对整个场景的全局配置，包括地图控件、场景蒙层、场景漫游、时序事件等； 效果预览区：针对图层参数修改，提供效果实时预览功能，所见即所得。

7.2.1.7 云安全服务

安全管控是云平台的重要组成部分，云安全服务为云用户提供多层面一体化的安全解决方案，从网络、服务器、应用、数据、安全管理和安全服务等多方面保护云上资产安全。云安全依托云计算的高弹性扩展和大数据分析能力，按照等保 2.0 三级防护要求建设。

等保：根据《GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求》第 3 级安全要求，满足安全通用要求和云计算扩展要求，进行定级、防护、测评及备案。应满足《GB/T 25070-2019 信息安全技术网络安全等级保护安全设计技术要求》第 3 级系统安全设计要求。产品应为安全自主可控产品（包括 CPU 和操作系统等）。

安全软硬件资源的授权需为永久授权，且病毒库、特征库等具备时效性的数据库需同时提供十年的免费离线更新服务。

7.2.1.7.1 态势感知

威胁态势感知是利用大数据，通过威胁态势感知系统从攻击者的角度，有效捕捉高级攻击者使用的 0day 漏洞攻击、新型病毒攻击事件和正在发生的安全攻击行为有效地展示，帮助客户实现业务安全可视和可感知。威胁态势感知系统是一个大数据安全分析平台，它通过机器学习和数据建模发现潜在的入侵和攻击威胁，从而解决因网络攻击导致数据泄露的问题，并通过溯源系统追踪黑客身份。

威胁态势系统可以实现以下目标：

支持对高级持续性威胁 APT 威胁攻击的检测。

实现对已知入侵威胁安全态势的感知；

实现对未知威胁安全态势的感知；

实现对恶意文件（Webshell、木马、恶意执行脚本）的态势感知；

实现对资产自身脆弱性的态势感知；

实现对云平台用户个人信息是否泄漏到外网（综合数据网等）的监控；

实现对业务系统的安全态势监控和展示。

作为一个集合了大数据和安全的跨界产品，态势感知系统不仅拥有强大的大数据分析和计算能力，而且通过机器学习，汇集全网安全数据和威胁情报，建立了完整的智能的安全威胁模型，并作用到百万客户的实际业务场景中。通过对海量数据的收集、分析

与展现，帮助客户获得无与伦比的全局可见性和安全智能性，从而抵御来自各个维度和领域的新型安全威胁。

态势感知用大数据分析的方法，用智能化的机器学习和建模分析，聚焦数据中心云计算用户面临的定向 Web 应用攻击、面向系统的暴力破解，黑客入侵行为，应用层主机层漏洞等多个方面的新威胁和新的安全趋势。

指标子项	具体要求
总览	提供整体安全威胁概览信息，包括防护资产状态、待处理风险告警、已处理风险等态势信息。
大屏展示	提供基于态势感知的大屏展示，包括资产、漏洞、基线、攻击来源、攻击分布等网络安全态势信息。
安全报告	通过创建分析报告，及时掌握资产的安全状况数据
应用白名单	支持应用白名单功能，针对未经白名单授权的程序进行监控告警，可监控进程名称、进程 ID 并提供解决方案，可进行一键处置。
攻击分析	支持定向攻击分析，比对云平台数据，分析出定向的应用攻击和定向暴力破解。
	支持异常流量分析，从流量中抓取异常流量，分析已知和未知攻击。包括发现异常的网络连接等。
	支持通过机器学习和数据建模发现潜在的入侵和攻击威胁，从攻击者的角度有效捕捉高级攻击者使用的 0Day 漏洞攻击、新型病毒攻击事件。支持但不限于以下模型的威胁检测：MySQL 提权和写 Webshell、主机侧挖矿程序检测、反弹 shell 等。
	支持防密码暴力破解攻击事件的发现，可对黑客进行暴力破解的行为进行实时检测，例如：支持对 SSH、RDP、Telnet、Ftp、MS SQL Server 等常见协议的登录行为检测。
资产中心	提供资产中心管理页面，包括服务器资产和云产品资产，展示的信息包括不限于防护状态、所属 vpc、风险类型等信息
采集性能	日志分析支持亿级数据的秒级检索能力：索引查询性能，在 10 亿条事件数据中，查询时间范围在 5 天以内，精确单条件查询事件，返回结果耗时不超过 3 秒。
日志采集	支持数据采集和线性扩容，支持 TB 级海量存储
日志保留	支持数据长期存储 180 天
威胁分析	支持客户威胁模型或威胁检测策略的自定义开发和运行
安全编排	支持对云原生安全产品，响应策略统管，告警统一响应处置，API 原生适配，版本同步迭代
告警管理	支持对告警进行处置和响应
事件管理	支持安全威胁事件的列表管理及详情查看
威胁情报	支持安全威胁指标的列表管理及详情查看，覆盖多种指标类型，并且可以自定义扩展：文件、URL、IP、域名等
工作空间	租户企业项目下，租户功能隔离，上述功能均在租户权限范围内管理；
安全建议	通过自动同步主机安全漏洞扫描数据，分类呈现漏洞扫描详情，支持查看漏洞详情，并提供相应漏洞修复建议；

指标子项	具体要求
	通过执行云服务基线扫描，检查基线配置风险状态，告警提示存在安全隐患的配置，并提供基线加固建议；

7.2.1.7.2 主机安全

主机安全支持自动化实时入侵威胁检测、恶意代码检测、漏洞智能修复、基线一键检查等功能，是构建主机安全防线的统一管理平台。

指标子项	具体要求
性能指标	业务高峰期对系统资源的影响：高峰 CPU 占用<5%，内存高峰占用<300M
	业务平稳期对系统资源的影响：平均 CPU 占用<1%，内存平均占用<200M
资产管理	支持展示进程、端口、账号、软件、中间件、自启动项和内核模块等维度的最新指纹信息和历史变动记录。（支持范围：账号、开放端口、进程、软件、自启动项）
入侵防御	支持威胁检测模块具备多种威胁检测模型，能够覆盖云上 95%以上的入侵事件。并按照操作系统、分析对象、攻击手法等维度进行分类，能够帮助用户快速了解云环境入侵事件
	支持网站后门防护功能，支持自动拦截黑客通过已知网站后门进行的异常连接行为，并隔离相关文件，有效清理隔离 php、asp、jsp 等类型的 webshell 后门。
	勒索防护提供对勒索诱捕以及数据恢复风险的监控能力。帮助用户拦截勒索病毒运行，排查备份习惯较差的资产，降低数据恢复风险。
	支持对常用登录地、登录 IP、登录时间、登录账号、web 目录进行自定义
	支持拦截勒索软件、挖矿程序、木马程序、蠕虫病毒、恶意程序、后门程序、DDoS 木马 、自变异木马、感染型病毒、黑客工具、漏洞利用程序、被污染的基础软件、Rootkit 等
	支持查杀的病毒类型：勒索病毒、挖矿程序、DDoS 木马、木马程序、后门程序、恶意程序、高危程序、蠕虫病毒、可疑程序、自变异木马等
	支持检测自动生成利用脚本
	支持安全策略工作模式设置，其中包括观察模式、拦截模式；
	支持自研的特征规则引擎、行为分析引擎、机器学习引擎以及权威的第三方特征规则库，可根据需要随时加载离线更新包、提高安全检出率和准确率；
	支持设置黑名单、白名单
	支持检测批量蠕虫挖矿脚本
	支持常见典型攻击、入侵的识别与防御，如：爆破、扫描、web 攻击、Webshell、反弹 shell、恶意程序、异常协议、数据泄密等；
基线检查	口令复杂度策略检测：支持口令复杂度策略检测和结果显示；
	经典弱口令检测：支持系统/应用账号的弱口令检测和结果展示，针对弱口令提示用户修改；
	风险配置检查：支持基于安全实践和等保合规检测风险配置，包括 Docker/Redis/Nginx/SSH/vsftp 等的风险配置，帮助用户识别不安全的配

指标子项	具体要求
	置项。
	基线策略管理：支持定义基线检查策略，包括新建/编辑/删除基线检测策略
主机运行安全检测	账户暴力破解防护：支持检测/阻断“尝试暴力破解”和“暴力破解成功”等暴力破解行为。
	风险账号检测：支持检测主机系统中的账号，列出当前系统中的可疑账号信息，帮助用户及时发现非法账号。
	漏洞利用检测：支持对 Hadoop/Redis 漏洞利用攻击进行检测和告警。
	关键文件变更检测：对于系统关键文件进行监控，文件被修改时告警，提醒用户关键文件存在被篡改的可能。
	文件/目录变更检测：对于系统文件/目录进行监控，文件/目录被修改时告警，提醒用户文件/目录存在被篡改的可能。
	进程异常行为检测：支持进程异常行为检测和结果显示，帮助客户及时发现行为异常的可疑进程。
	网站后门(Webshell)检测 ：支持检测云服务器上 web 目录中的文件，判断是否为 Webshell 木马文件，支持检测常见的 PHP、JSP、JSPX 等后门文件类型。
	反弹 Shell 检测：实时监控用户的进程行为，及时发现进程的非法 Shell 连接操作产生的反弹 Shell 行为。
	异常 shell 检测：检测系统中异常 Shell 的获取行为，包括对 Shell 文件的修改、删除、移动、拷贝、硬链接和访问权限变化。
	Crontab 可疑任务检测：支持自启动变更检测和结果显示，及时发现异常自启动项，帮助快速定位恶意程序。
	高危命令执行检测：实时检测当前系统中执行的高危命令，当发生高危命令执行时，及时触发告警
	root 提权检测：支持检测利用 SUID 程序漏洞/内核漏洞提取的异常行为，支持检测文件提权的异常行为
	rootkit 检测：支持检测服务器是否感染 rootkit 程序。
	虚拟机逃逸检测：支持虚拟机逃逸检测，包括敏感命令执行、敏感文件访问和异常端口访问。
	恶意程序检测：支持恶意程序（包括后门、木马、病毒、挖矿和蠕虫等）检测、隔离查杀及可视化结果显示。
安全响应	支持对告警事件进行手工处理、忽略、加入登录白名单和隔离查杀文件。
	支持恶意程序/进程的隔离查杀、通过文件隔离箱取消隔离查杀和解除拦截 IP
勒索病毒防护	勒索签名检测：支持基于勒索签名检测/阻断已知勒索病毒。
网页防篡改	核心文件防篡改，包括静态网页文件篡改等：支持静态防篡改检测、防护、备份/恢复，防止服务器中的静态文件被篡改。
	支持主机软件安装的资产信息，包括具体软件资产名称、软件版本、软件安装目录、最新采集时间等信息
白名单管理	支持通过告警和登录白名单进行告警消减、告警处置
二次认证	支持对云服务器登录行为进行二次认证。

指标子项	具体要求
安全报告	支持安全报告（包括安全日报、周报、月报和自定义报告）的创建、编辑、复制、生成、显示和下载，并支持自动/手工发送安全报告邮件。
策略管理	支持检测策略的修改和查看，可以自定义检测策略配置与并下发，能够为每组或每台主机灵活配置检测策略，便于精细化安全运营。

7.2.1.7.3 容器安全

指标子项	具体要求
容器资产管理	支持清点并展示本地镜像版本、大小、类型、关联主机数、关联容器数、组件数、创建时间等信息。
	支持清点并展示容器节点名称、防护状态、节点状态等信息。
	支持清点并展示进程路径、启动参数、文件权限、文件 HASH、开放端口、软件版本、容器名称等信息。
	支持清点并展示应用、软件、容器、网络相关信息；
	支持清点并展示中间件、数据库、文件应用相关信息；
镜像安全	支持扫描容器镜像，包括私有镜像、官方镜像，以及节点中所有正在运行的镜像，支持发现镜像中的漏洞并给出修复建议。
	支持对容器私有镜像、官方镜像进行基线检查并给出修复建议。
安全策略管理	支持容器进程白名单，阻止异常进程、提权攻击、违规操作等安全风险事件的发生。
	支持文件保护，可将容器中关键的应用目录设置只读保护以防止黑客进行篡改和攻击。
运行时安全	支持检测容器内发起的高危系统调用检测，识别可能引起安全风险的 Linux 系统调用，如“open_by_handle_at”“ptrace”“setns”“reboot”等。
	支持基于容器进程白名单和进程行为特征/文件指纹检测异常的容器进程。
	支持对容器启动配置选项和启动权限异常进行检测，如特权容器启动、设置 Capabilities 权限过大、内核 seccomp 模式未启用、危险目录挂载映射等。
	支持检测违反安全策略的容器文件异常访问或敏感文件访问。
	支持检测漏洞逃逸攻击和文件逃逸攻击，包括 shocker 攻击、进程提权、DirtyCow 和文件暴力破解等。
	支持设定准入启动策略阻断非法容器启动。

7.2.1.7.4 数据库审计

数据库审计系统实现了对云端自建数据库、数据库访问的精确审计及准确地应用用户关联审计，并具备风险状况、运行状况、性能状况、语句分布的实时监控能力。

数据库审计系统通过数据库化的界面语言、智能化的协议识别、可视化的运行状况呈现、可交互可下钻的风险追踪能力，完美实现快速部署、方便维护的云数据库审计。

指标子项	具体要求
审计报表	支持预置报表模板，包括数据库安全综合报表、数据库安全合规报表、SOX-萨班斯报表、数据库服务器分析报表、客户端 IP 分析报表、DML 命令报表、DDL 命令报表、DCL 命令报表。
性能指标	不少于万条/秒吞吐量，千万条/小时的入库速率，十亿条在线 SQL 语句存储，百亿条归档 SQL 语句存储。可扩展实例数量。
支持协议	支持本项目采购的所有数据库（包括但不限于 AP 库、TP 库、内存数据库、数据计算组件涉及的非关系数据库等等）产品的审计。
	支持国产主流数据库。
权限管理	支持系统管理员，安全管理员，审计管理员权限分离（三权分立），满足审计安全需求，并支持统一身份认证管理。
隐私数据保护	用户可以通过内置规则或自定义规则对审计日志存储和展示的敏感信息脱敏
审计功能	支持通过访问来源信息：客户端 IP、端口、数据库名称、数据库用户、访问工具、主机名称、MAC 地址的方式进行审计。

7.2.1.7.5 安全管理中心

指标子项	具体要求
态势总览	提供资产的安全风险评估 资产威胁告警统计&TOP 排名 漏洞统计&TOP 排名 安全基线检查结果&TOP 排名 和近 7 天安全评分数据趋势等统计信息
安全大屏	综合态势大屏，威胁响应大屏，安全值班大屏等
资产管理	支持资产与安全风险要素关系：资产与弱配置、资产与漏洞、资产与威胁告警、资产与预期事件等；
基线检查	支持弱配置详情解读，及修复指导；
漏洞管理	支持漏洞单管理；
	支持按漏洞汇聚，展开到 CVE、资产；
告警管理	支持便捷时间窗查询，支持任意字段查询；
	支持告警单操作：增删改、导出、关单、转事件、威胁阻断；
	支持自动接入威胁检测模型告警
	支持自动接入云安全产品告警：主机安全、web 应用防火墙、云防火墙、Ddos，统一管理，并同步状态；
	支持关联剧本/流程，自动研判降噪；
	支持自动通知
	支持导入三方安全产品告警
告警类型	支持主机高危命令、运维通道异常行为、应用漏洞攻击、网络边界探测等多种告警类型

指标子项	具体要求
	告警类型明确关联 Mitre 矩阵
	支持自定义扩展类型
	支持根据不同告警类型，区分不同的交互界面
	支持根据不同告警类型，定义不同的响应剧本
事件单管理	支持便捷时间窗查询，支持任意字段查询；
	支持事件单操作：增删改、导出、关单、威胁阻断；
	支持关联剧本/流程，自动取证、辅助研判调查；
	支持定义事件阶段，并指定 SLA
	支持自动通知
情报管理	支持便捷时间窗查询，支持任意字段查询；
	支持自动从告警、事件中提取情报画像，并自动更新描绘；
威胁模型库	身份及运维安全类：凭据泄露、异常登录、越权访问等；
	网络安全类：异常外联、端口扫描等；
	应用安全类：Log4J 漏洞成功利用、漏洞扫描等；
	主机安全类：高危命令、漏洞提权等；
	数据安全类：异常数据流动等；
威胁分析	指定字段进行检索，筛选，过滤
	支持 SQL 检索
剧本编排	支持定时调度触发
	支持对象创建及更新时自动触发，支持与或非条件筛选；
	支持多流程并行
流程编排	支持流程定义出参入参
	支持设置失败重试，全量重试
	支持流程调试，逐个节点断点，变量监视、调试参数模板等；
	支持入参、出参变量、支持关联对象获取成员变量、支持自定义临时变量；
	支持流程版本管理，版本启用及停用管理；
	支持导入导出：

7.2.1.7.6 云防火墙

云防火墙可统一管理南北向的流量，提供访问控制、流量分析等功能，全面保护网络安全。云防火墙通过拓扑图直观地展现资产以及资产的访问关系。无需配置，开通服务后就可了解业务的分区、分组、资产、资产间的访问关系，以及用户流量的聚类分析。支持流量可视分析，最大程度保证策略的正确性。

指标子项	具体要求
云原生	云平台原生的云防火墙服务，具备统一的 Console 管理界面、自动化

指标子项	具体要求
	实例发放能力。
性能指标	单实例最大支持：最小并发连接数（HTTP1.1）20 万，每秒新建连接数 (HTTP1.1)1 万/秒。
	吞吐量不少于 100Mbps
场景支持	提供云上南北向防护； 提供云上东西向防护；
访问控制	支持基于五元组、黑白名单设置访问控制策略。
	支持基于域名/泛域名的访问控制。
	支持 Internet 边界访问控制，同时控制入流量和出流量的访问。
入侵防御	支持入侵防御（IPS）功能，包括检测模式与阻断模式。
	提供入侵防御引擎对恶意流量实时检测和拦截，防御木马蠕虫、注入攻击、漏洞扫描、网络钓鱼、暴力破解等攻击。
	支持对 IP 地址组、 黑名单、白名单设置 ACL 访问控制策略。
流量分析	支持互联网到业务的访问流量分析。
	支持业务向外的主动外联分析。主动发现云服务器主机的异常行为
日志存储	支持入侵事件日志、流量日志和访问控制日志等类型日志记录
扩展性	支持 FWaaS 化部署，无需改变客户网络结构，即开即启使用
	支持高可靠，集群化部署，支持根据业务发展平滑扩展性能和策略数量。

7.2.1.7.7 云堡垒机

云堡垒机是平台一个核心系统运维和安全审计管控平台。堡垒机集中了运维身份鉴别、账号管控、系统操作审计等多种功能。基于协议正向代理实现，通过正向代理的方式实现对 SSH、远程桌面、及 SFTP 等常见运维协议的数据流进行全程记录，并通过协议数据流重组的方式进行录像回放，达到运维审计的目的。云堡垒机支持云化部署方式，满足安全组件和业务云化需求。

指标子项	具体要求
身份认证	支持 AD 域、RADIUS、LDAP 用户账号远程认证。
权限控制	支持按照用户、用户组、资源账户、账户组，建立用户对资源的访问控制授权，支持通过配置访问控制策略、命令控制策略实现对资源不同维度的控制。
账户管理	支持纳管弹性云服务器资源。
密码策略	支持用户安全策略功能，如密码最小长度、密码使用限期、密码复杂度要求、密码重复策略、密码锁定策略等
审计记录及检索	支持会话录像在线回放、定位回放及下载后使用官方专用客户端离线回放
高危指令审计	支持设置命令控制策略对关键操作进行管控，当进行敏感、高危操作时，触发的系统响应需至少包括动态授权、强制阻断、告警及高危指令的二次审查。

指标子项	具体要求
密码管理	支持按设备、系统账号、计划执行时间、改密周期、密码策略、改密结果发送等生成详细的改密计划，到期自动执行；
	支持随机生成不同密码的密码策略、支持伪随机数生成器，并能严格遵守密码强度设置；
数据检索	支持对 RDP 屏幕文字内容、标题窗口、键盘输入的记录和搜索定位
系统用户管理	支持多种认证方式：本地静态密码认证、RADIUS 认证、LDAP 认证、AD 域认证；
金库授权	支持金库授权模式，配置金库授权后，运维人员若需访问核心资源，支持多级授权方式，，通过认证后才能访问核心资源。
协同会话	支持邀请多人进入同一会话，协同进行运维工作、技术共享。
运维方式支持	Web 访问方式：支持使用浏览器直接调用 H5 控件实现运维操作；支持 Web 页面调用 DB2cmd、PLSQL、Toad、Mysql、Sqlplus、Isqlw、SqlAdvantage、PowerBuilder、SqlPlusW、Sqlldr、mstsc、Xshell、SecureCRT、Putty、winscp、flashFXP、FileZilla、Netterm、LeapFTP 等运维客户端工具
双因子认证	支持双因子组合认证，可以将两种认证组合为全新的双因子身份认证方式，而非一种双因素认证。
国密算法	支持国密算法，可在传输、存储环节使用国产算法加密，支持使用国密智能密码钥匙做身份认证。提供包括 20 个智能密码钥匙，含具有资质国密证书

7.2.1.7.8 Web 应用防火墙

Web 应用防火墙，能够保护网站的应用程序避免遭受常见 Web 漏洞的攻击。这类攻击既有诸如 SQL 注入、XSS 跨站脚本等常见 Web 应用攻击，也有 CC 这种影响网站可用性的资源消耗型攻击。防御常见威胁：针对 GET、POST 常见 HTTP 请求，提供不同规则策略，进行 SQL 注入、XSS 跨站、Webshell 上传、后门隔离保护、命令注入、非法 HTTP 协议请求、常见 Web 服务器漏洞攻击、核心文件非授权访问、路径穿越、扫描防护等安全防护。同时，它也允许根据网站实际业务制定精准的防护策略，用于过滤对网站有恶意的 Web 请求。

指标子项	具体要求
基础防护 域名防护	针对 OWASP top 攻击进行安全防护，包括 XSS、SQL 注入、命令注入、CSRF、代码注入、远程溢出攻击、Webshell 检测（上传木马）等；支持 CC 防御、数据防爬虫、自定义防护策略等；使用双引擎，语义分析+规则防护，误报率更低；
	域名（泛域名、一级域名、二级域名等各级域名）/IP 防护
HTTP/HTTPS 业务防护	WAF 可以防护 HTTP/HTTPS 业务，通过对 HTTP/HTTPS 请求进行检测，识别并阻断 SQL 注入、跨站脚本攻击、网页木马上传、命令/代码注入、文件包含、敏感文件访问、第三方应用漏洞攻击、CC 攻击、恶意爬虫扫描、跨站请求伪造等攻击，保护 Web 服务安全稳定。

指标子项	具体要求
支持 WebSocket/WebSockets 协议	WAF 支持 WebSocket/WebSockets 协议，且默认为开启状态。
非标端口防护	Web 应用防火墙除了可以防护标准的 80，443 端口外，还支持非标准端口的防护。
防敏感信息泄露规则	该规则可添加两种类型的防敏感信息泄露规则： 敏感信息过滤。配置后可对返回页面中包含的敏感信息做屏蔽处理，防止用户的敏感信息（例如：身份证号、电话号码、电子邮箱等）泄露。 响应码拦截。配置后可拦截指定的 HTTP 响应码页面。
全局白名单(原误报屏蔽)规则	针对特定请求忽略某些攻击检测规则，用于处理误报事件。
网站反爬虫规则	动态分析网站业务模型，结合人机识别技术和数据风控手段。 特征反爬虫 自定义扫描器与爬虫规则，用于阻断网页爬取行为，添加定制的恶意爬虫、扫描器特征，使爬虫防护更精准。 JS 脚本反爬虫 通过自定义规则识别并阻断 JS 脚本爬虫行为。
防绕过	支持 11 种编码还原，攻击绕过难度更大，至少支持对 web 攻击的 url_encode，Unicode 编码，xml 编码，C-OCT 编码，十六进制编码，html 转义编码，base64 编码，大小写混淆，javascript、shell、php 等拼接混淆编码的还原能力
CC 防护	支持 IP/Cookie/Referer 的 CC 防御，用户可选粒度更细，更灵活
爬虫检测	支持恶意爬虫检测能力；
IP 黑白名单	支持自定义 IP 黑白名单、精准访问防护规则；
网页防篡改	支持网站静态页面防篡改能力；

7.2.1.7.9 日志审计

指标子项	具体要求
日志管理	支持采集租户 VPC 内数据，支持对日志、告警、漏洞等安全数据自动化租户和资源标识，并支持云外安全数据采集；
	采集任务支持多节点分布式采集，可根据需求弹性扩容
	云服务安全日志开箱即用，支持 web 应用防火墙，云防火墙，主机安全、数据库审计等云服务安全日志预置接入
	支持三方产品日志采集，可接入任意三方数据源，对接协议支持 TCP、UDP、HTTP，对接格式支持 json、syslog、keyValue、csv、任意自定义格式
安全日志保留	云平台日志支持完整保留 180 天，满足等保等审计要求的保留时长
日志备份	支持日志转存备份，对象存储、云硬盘等；支持存储容量空间告警。
安全日志检索	支持类 SQL 检索，检索结果即支持表格视图，也支持原文 Json 视图；
	通过关键字、条件表达式、时间范围进行快速点击检索，筛选，过滤；
安全数据导出	支持将采集到的日志，转发至三方的日志审计或者安全平台

指标子项	具体要求
	转发的节点，部署在租户 VPC 内，一键安装，可转发至云外，或者租户 VPC 内
	导出协议：支持 TCP、UDP、HTTP （HTTP 有限支持）
管理与部署	基于云管的统一管理入口：云原生服务，统一管理入口，统一用户体验；
	自动化交付部署：全区域，SaaS 化服务自动部署，不用每个租户单独部署；便于后续运维；
	快速弹性扩展：支持集群横向弹性扩展；
	运维监控统一对接至云管平台；
	支持单账号单区域、单账号跨区域、跨账号单区域和跨账号跨区域的数据统一托管
	支持单账号单区域、单账号跨区域、跨账号单区域和跨账号跨区域的权限统一托管，支持不切换页面的统一安全管理
	基于云管的统一管理入口：云原生服务，统一管理入口，统一用户体验；

7.2.1.7.10 漏洞扫描

漏洞扫描旨在帮助企业自动化发现、维护 IT 资产风险，从漏洞安全、合规检测以及外部威胁情报分析等多个维度持续监控企业安全。根据企业的已知资产自动、快速、准确检测发现企业的未知资产及所有资产的漏洞，帮助企业更快速、更全面、更智能地管理企业的 IT 资产和资产安全风险。

指标子项	具体要求
功能要求	支持应用漏洞、运维安全漏洞、弱口令、Web 漏洞、基线监控、合规漏洞等风险检测。
	支持 VPC 侧扫描自动导入虚拟云主机资产，可手工添加扫描目标 IP 。
	支持主机资产管理，采用 TCP_SYN、ICMP_ECHO、UDP、TCP_ACK、SCTP 等多种方式，同时支持 IPV6 扫描，并支持探活端口设置，全天候巡检发现资产更新并展示
	支持主机资产的内外网识别，同时获取资产存活/更新状态、关联域名、操作系统、端口、服务、中间件、地理位置、漏洞信息、指纹、来源、扫描时间等信息。
	支持以饼图、柱状图、趋势图等形式展示资产综合状况，支持从资产类型、漏洞类型、主机存活状态、服务类型等角度展示。
	支持漏洞闭环管理，能对漏洞进行确认、忽略。
	支持漏洞风险 TOP N 展示，包括但不限于应用漏洞、运维安全风险、风险资产、弱口令等。
	支持漏洞风险分析，包括但不限于风险概述、风险地址、风险类型、风险描述、风险危害、风险细节、修复建议以及原始请求与响应等信息。
	支持突发事件应急检测，能够针对单个或多个漏洞进行指定资产范围内的风险发现。
	支持自定义导出资产综合报表和资产报表，导出格式包括但不限于 PDF、

指标子项	具体要求
	Word、Html、Excel 等。
	支持自定义资产白名单，系统对白名单内资产不进行资产监测或风险扫描。
	支持设置资产巡检周期，自定义扫描周期、扫描开始/结束时间、扫描速率、探活发包协议、端口策略、漏洞类型、User-Agent 等信息。
	支持资产发现和漏洞扫描的可视化展示，显示巡检周期数、巡检进度、巡检状态等。
	支持资产导入功能，包括域名资产、主机资产、网站资产，实时查看导入进度 。
	支持资产更新分析，自动收集资产更新前后信息，并针对更新内容进行重点对比展示。
	支持资产状态检测，资产自动收集、识别资产上线、下线和更新等状态。
	支持资产风险分析，包括但不限于未修复、已修复风险、已确认、待确认、已忽略等不同风险维度展示，同步展示漏洞数量趋势、风险生命周期等信息。
	支持运维弱口令检测功能，包括 mysql、SSH、FTP、Redis 等主流服务口令检测。弱口令字典可以自定义设置。
	支持通过自定义分组、负责人、手机、邮箱、标签、资产来源及变动等属性对资产进行业务化管理。
	支持通过资产指纹进行漏洞分析，并从资产的类型、服务版本、漏洞类、漏洞严重程度等多个维度进行关联分析。
	漏洞标准兼容 CVE、CNVD 等 。
	系统漏洞库能够覆盖常见的操作系统漏洞、软件漏洞、最新的网站框架应用漏洞等。能够针对操作系统 以及 Web 漏洞进行检测。
	针对厂商各类产品的漏洞，支持漏洞原理性插件检测，分析风险危害并给出相应建议。

7.2.1.7.11 安全组

安全组是一种有状态的包过滤功能虚拟防火墙，用于设置单台或多台云服务器的网络访问控制，是重要的网络安全隔离手段；

功能子项	具体要求
功能要求	创建多个安全组，并给每个安全组指定不同的规则
	每个虚拟机实例分配一个或多个安全组，按照规则确定：哪些流量可访问虚拟机实例、虚拟机实例可以访问哪些资源
	配置安全组，以便只有特定的 IP 地址或特定的安全组可以访问虚拟机实例

7.2.1.7.12 流量安全监控

指标项	指标要求

全流量检测	支持大流量检测，支持典型应用协议识别，如：HTTP/TCP/UDP/DNS/SSH 等。
入侵检测	支持常见典型攻击的识别与防御，如：爆破、扫描、Web 攻击、Webshell、反弹 shell、恶意程序、异常连接、异常协议、数据泄密等。
安全策略	支持工作模式设置为观察模式或拦截模式。
黑白名单	支持按照 IP 地址或者 IP 地址段设置黑名单、白名单。
行为审计	支持用户访问行为审计，包括中间件应用访问审计、高危协议请求连接审计、黑客工具连接审计；行为审计对应的字段包括发生时间、危险等级、告警可信度、项目 ID、租户名、规则 ID、命中规则名称、攻击源 IP、攻击源端口、被攻击 IP、被攻击端口、传输协议、应用协议、方向的字段。
规则特征库	支持特征规则引擎、行为分析引擎、机器学习引擎以及权威的第三方特征规则库，可根据需要随时加载离线更新包，提高安全检出率和准确率。
威胁情报集成	支持地理位置信息库，方便客户通过地理位置判断攻击源。
ATT&CK 攻击模型	支持 ATT&CK 矩阵视角分析攻防过程，基于权威机构的攻防全过程宝典，帮助掌握黑客的策略和技术，进一步辅助分析检测或阻止攻击。
安全可视化图表	支持查看详尽的安全可视化图表，从检测和响应两方面深入掌握攻防全过程的关键数据，包括告警响应趋势、告警总数、检测总数、受害 IP 数、攻击 IP 数、告警风险类型分布、告警可信度分布、告警危险等级分布、告警趋势、攻击者分布 TOP5、攻击类型 TOP5、受害 IP TOP5、攻击者（受害 IP 维度） TOP5、攻击响应数、阻断攻击数、封禁 IP 数、新增白名单数、IP 状态分布、攻击响应分布、阻断类型分布、攻击响应趋势、阻断 IP 分布 TOP5、阻断 IP TOP5 展示。
响应方式	支持日志查看和检索；支持攻击告警；支持阻断拦截；支持提供 API 供第三方调用阻断。
日志及报表	支持流量日志、攻击日志的查找、分析；基于威胁事件、流量统计、协议统计等生成报表；攻击日志可关联显示被攻击主机所属的用户名、项目 ID、命中规则、五元组、攻击 payload 等信息。
高可靠性	探测引擎支持集群部署，支持 Bypass 或其他方式；管理节点支持集群部署。

7.2.1.7.13 数据脱敏

数据库脱敏采用专门的脱敏算法对敏感数据进行屏蔽、随机替换、乱序处理和加密，将敏感数据转化为虚构数据，隐藏真正的隐私信息，为数据的安全使用提供基础保障。同时，在不改变业务系统逻辑的前提下，保证脱敏后的数据保留原数据的特征和分布，使企业低成本、高效率、安全地使用生产环境的隐私数据。数据库脱敏自动识别和管理敏感数据，提供灵活的策略和脱敏方案，提供高效、可并行的脱敏能力。数据库脱敏帮

助企业快速实施敏感数据脱敏，同时保证数据的有效性和可用性，使脱敏后的数据能够安全地应用于测试、开发、分析和第三方使用环境中。

指标项	具体要求
数据库类型	支持安全自主可控数据库及数据仓库；
脱敏方式	系统支持自定义、图形化操作的脱敏规则和脱敏方式，支持 UNICODE 标准、中文等字符编码。支持数据库到数据库、数据库到文件、文件到文件、文件到数据库等多种脱敏方式。
敏感数据自动发现	1、系统应支持敏感信息的自动发现能力，系统具有内置敏感数据特征库，能对身份证、通用证件号、银行卡号、电话号码（手机、座机）、中文姓名、中文地址、企业名称、日期、税号、email 地址、金额、统一社会信用代码、组织机构代码、工商注册号、ip 地址、mac 地址、车牌号、敏感信息自动识别。 2、系统能读取数据库或 txt、csv 等文件内容，根据内容和内置敏感数据特征规则发现敏感数据。 3、系统支持一个单元格的数据按位拆分或按字符拆分成多种敏感数据类型进行发现 4、系统支持按照数据字典进行敏感数据发现的能力，凡是字段中数据在数据字典内占有一定比例的，则该字段被发现为敏感字段。 5、支持以文件导入的方式，将客户预先定义好的敏感字段导入至系统中。 6、支持在系统前台界面设置自定义敏感类型的发现函数，函数可以采用 Python，PHP，JavaScript 等一种或多种。
脱敏方案	支持灵活的脱敏方案管理，脱敏方案与脱敏任务不绑定。对脱敏方案进行调整、修改时不影响与之相关的脱敏任务，不需要删除与脱敏方案相关的字段发现以及脱敏任务。
数据子集管理	可以在脱敏流程配置中，调用定义好的子集规则，具有抽取多表间关联的子集抽取功能。
脱敏任务管理	1、支持对脱敏任务进行停止、启动，并且支持任务并发，充分利用系统资源，提高脱敏效率。 2、脱敏任务可兼容执行过程中遇到的异常情况，支持跳过异常数据继续执行任务，包括对异常数据的丢弃、填充、置空处理。
脱敏对象	在执行脱敏任务时，除了要将数据脱敏至目标库，还需要将源库中约束和敏感表上其他对象一并迁移至目标库，包括序列、视图、包、函数、存储过程、索引、约束、触发器等。
定时任务	系统支持定时、定期自动执行发现任务和脱敏任务的功能。支持按照日期、时间对任务进行定时。
增量脱敏	系统支持基于时间类型字段或自增字段的数据增量脱敏功能。
数据对比	系统支持通过查询单表数据实现脱敏后数据对比功能。
文件脱敏	1、支持无中间数据库情况下脱敏 dmp 文件 2、支持对 Excel、CSV、DEL、TXT 文件脱敏。
脱敏模板	支持定义文件脱敏模板，用户上传需要脱敏的文件后通过选择模板即

	可完成敏感数据确认、脱敏算法选择、脱敏方案选择等任务，便于快捷地对文件进行脱敏。
同义替换	使用相同含义的数据替换原有的敏感数据，如姓名脱敏后仍然为有意义的姓名，住址脱敏后仍然为住址。
部分数据遮蔽	将原数据中部分或全部内容，用“*”或“#”等字符进行替换，遮盖部分或全部原文。
数据关联	脱敏算法保持数据关联性，能够保持同一数据库中不同表字段之间的数据关联性，也能保持不同数据库之间的表字段间的数据关联性。
自定义函数	1、对有特定业务需求的敏感数据可通过自定义发现函数实现和自定义脱敏函数实现。 2、支持在系统前台界面配置自定义函数设置脱敏算法，函数可以采用 Python，PHP，JavaScript 等一种或多种。
部署模式	旁路部署：网络可达即可。
脱敏数据安全性	系统不允许真实生产数据落地，不能存储生产数据；并提供审计报告，包括用户信息、脱敏配置信息、任务信息等。

7.2.1.7.14 数据水印

指标项	具体要求
数据水印	1、支持针对 pdf、word、excel 格式的文件提供添加和提取水印的功能。 2、支持版权证明：嵌入数据拥有者的信息，保证资产唯一归属，实现版权保护。 3、支持追踪溯源：嵌入数据使用者的信息，在发生数据泄露事件时，追踪其泄露源头。 4、支持明暗双重水印，具备高鲁棒性，可检测性强、不易被篡改等特性。 5、支持数据库水印，能对本项目采购的所有数据库（包括但不限于 AP 库、TP 库、内存数据库、数据计算组件涉及的非关系数据库等等）数据源进行水印嵌入和提取，具备高鲁棒性，可检测性强、不易被篡改等特性。
数据资产目录	1、支持以数据库、数据表为单位统一管理数据库资产。 2、支持从业务域和数据类型两个维度查询数据目录信息。 3、支持对数据目录进行检索、过滤、查看详情、查看关系。 4、支持手动、定期发起元数据扫描任务，自动拉取元数据信息。 5、支持对数据进行分组管理、查询数据列表。

7.2.1.7.15 蜜罐系统

蜜罐基于伪装欺骗技术，通过在攻击者入侵的关键路径上部署诱饵和陷阱，诱导攻击者进入与真实网络隔离的蜜网，让攻击者在蜜网中攻击伪装的服务、获取虚假的数据，进而完整记录攻击者行为，捕获高级未知攻击，并且对攻击者做取证和追踪溯源，为防守方提供先人一步的主动防御手段，保护真实资产，提升主动防御的能力。

功能子项	具体要求
沙箱仿真	支持 ssh、redis、ftp、samba、memcahed、portcheat、momgoob、telnet、mysqlcheat、postgresql、ADB 等高交互系统服务沙箱。
	支持组合服务构建沙箱：创建沙箱时，支持选择多个服务进行组合，保障沙箱最大程度的灵活性；关联同网段空闲 IP，可绑定当前沙箱的所有服务。
	支持用户自行拓展沙箱的类型及数量，基于 docker 镜像制作沙箱，可自定义配置用户名、密码、系统名称、系统 LOGO 等。
	支持增、删、停、重置、编辑沙箱内容，沙箱可关联同网段多个空闲 IP，无需安装 agent 代理。
	支持调节行为灵敏度；支持自定义邮件告警级别；支持开启关闭溯源能力，自定义位置插入溯源组件。
	支持在新建沙箱时，向沙箱中注入脱敏数据，增加沙箱的真实性。 支持为 web 沙箱配置敏感目录，在该目录下生成普通配置文件、数据库配置文件、木马文件等；
诱饵感知	支持制作反制木马，用户自定义上传反制程序并关联沙箱，伪造敏感信息，诱骗攻击者进行下载。
	支持 PC 诱饵发布功能，包括网页浏览记录、网站登录密码、RDP 连接记录、登录域凭据、伪造新用户文件夹、伪造文件等。
	支持对已有文件 Word/Excel/PPT 加工，散布虚假信息到内网各处，感知攻击者访问行为。
	支持部署在 Kubernetes 场景，以 pod 的形式部署在 K8S 集群中，监测 K8S 集群中的攻击行为。
溯源反制模块	支持对黑客溯源功能，分析黑客的身份信息和设备指纹信息，包括 IP 地址、社交网站真人身份、设备指纹、操作系统、浏览器等。
	支持攻击反制功能，可以反向控制攻击者设备，获取对方设备信息，进行交互式反制操作；可获取设备配置信息、网卡信息、IP 信息、用户信息、进程信息、系统信息、桌面文件等；支持命令执行、文件上传下载、电脑截屏、摄像头拍照等操作，支持获取 qq、wechat、手机号、Git、Email、iphone 设备信息、浏览器保存的 URL 及对应的用户名等应用的用户 ID、cobaltstrike、xshell、navicat 等关键数据，便于身份溯源。
	支持 VPN 欺骗：以沙箱的形式发布到互联网，沙箱模拟真实的 VPN 服务，黑客从互联网获取 VPN 证书并成功登录后，可直接访问蜜网沙箱群。
行为记录	支持基于 ATTCK 的攻击事件回放，并以时间轴的方式展示重点攻击手法及事件，支持从攻击时间、攻击资产、攻击手法、来源 IP、事件类型等进行筛选。
	支持记录攻击者所有行为，并能识别真人与扫描工具
	支持记录攻击者上传的恶意文件，并分析其文件类型、MD5 等判断其是否为恶意木马，支持 VirusTotal 鉴定、AntiVirus 恶意文件鉴定等。
管理功能	账号权限分离，提供超级管理员、管理员、普通用户、审计员角色权限。
	支持扩展功能开关，包含 post 内容捕获、攻击源探测、逃逸检测、攻击反制、pcap 包下载等操作。

7.2.1.8 商用密码服务

商密：按照《GB/T 39786-2021 信息安全技术信息系统密码应用基本要求》三级要求，实现密码应用。产品应为安全自主可控产品，满足国产商用密码技术，达到《GB/T 37092 信息安全技术 密码模块安全要求》二级及以上安全要求。

7.2.1.8.1 密码服务管理平台

功能子项	具体要求
兼容性	1、产品及其依赖项满足《GB/T 36572-2018 电力监控系统网络安全防护导则》相关要求，应实现自身的安全，应安全、可控、可靠。 2、产品及其依赖项满足《GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求》3 级。
本体安全	1、产品及其依赖项满足《GB/T 36572-2018 电力监控系统网络安全防护导则》相关要求，应实现自身的安全，应安全、可控、可靠。 2、产品及其依赖项满足《GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求》3 级。 3、可限制仅特定地址登录； 4、远程管理设备时，应建立安全的通信协议； 5、支持国密双因子身份鉴别、应配置复杂口令并开启定期强制改密，配置国密 Ukey 数≧3；
服务调度	1、支持对服务器密码机等密码设备密码资源统一调度，为上层系统及应用提供按需高效、弹性可扩展的密码服务； 2、支持提供密码服务的基础管控能力，包括密码运算资源映射管理、密码资源弹性分配、密码资源灵活控制等功能； 3、支持资源动态分配，利用负载均衡技术实现虚拟化实例对密码资源占用的动态分配； 4、支持向业务和云平台应用（包括平台和租户侧）以及云平台本体提供统一丰富的密码功能接口，满足各种场景下的密码应用需求。
数据加解密	1、支持基于国产商密算法、国际密码算法的对称加解密、非对称加解密等服务功能。 2、支持重要数据（鉴别数据、重要业务数据、日志数据、访问控制信息）加解密功能。 3、支持数据库加解密服务功能，可应用于国产数据库。 4、支持对称算法的传输数据或文件加密、解密服务，支持使用公钥加密会话密钥、会话密钥加密数据的方式对传输数据或文件进行加密。 5、支持基于对称算法对结构化数据或文件的安全存储进行加密和解密。 6、支持对称密钥、非对称密钥的申请服务，申请对称密钥时，支持公钥加密输出密文或采用数字信封的方式加密输出。
签名验签	1、支持可信根证书管理，可同时采信多个厂商 CA 根证书。 2、可同时配置多条证书链，验证不同 CA 系统签发的数字证书。 3、提供证书解析功能， 获取证书中的任意主题信息以及扩展项信息。 4、实现基于数字证书的身份认证，支持不同 CA 的证书验证，提供 CRL/OCSP 等多种方式的证书有效性验证。

功能子项	具体要求
	5、支持 PKCS#1、PKCS#7 Attach、PKCS#7 Dettach、PKCS#7 数字信封、XML 等标准格式的数字签名。 6、支持对文件的数字签名和数字签名验证功能。
密钥管理	1、支持对密钥的全生命周期管理功能，支持密钥的生成、存储、备份、恢复、销毁、归档等功能。 2、支持 SM1、SM2、SM3、SM4、SM7、SM9 等国产密码算法。 3、提供创建外部密钥功能，支持将用户自有密钥加密导入密钥管理服务。 4、支持通过密钥版本化和定期轮转来加强密钥使用的安全性，提供应用完全透明的密钥自动轮转能力。 5、支持应用管理，支持密钥授权给指定应用。
平台管理	系统管理： 1、系统管理应提供用户管理、角色管理、授权管理、系统日志等管理功能。 2、用户管理应支持用户的添加、编辑、USB Key 绑定、重置口令、删除等操作。 3、角色管理支持角色的添加、编辑、删除等操作。 4、系统日志应支持日志的查看与下载。 资源总览： 1、提供统一的管理入口，统一管理密码服务资源和密码计算资源。 2、支持对密码服务管理平台、密码资源的运行情况监控，包含密码资源使用状态、业务资源使用状态和运行状态； 3、应支持密码资源态势监控，平台级管理员可监控对象应包括：密码服务调用概况和调用历史、密码计算资源运行概况、密码服务资源运行概况、密码服务分类分布概况和调用分布概况，支持 Web 大屏方式展示。 4、应支持密码服务资源监控，监控类型分为资源监控和业务监控，资源监控指标应包括：密码服务实例的处理器、内存、网络流量；业务监控指标应包括：密码服务整体和类别的 TPS、平均响应值。支持按时间区间统计实时和历史监控数据的能力。 密码服务管理： 1、密码服务管理支持服务的详情查看和监控操作。 2、支持密码服务实例的配置、监控、升级、重启、关闭、释放、备份和恢复的功能。 3、支持密码服务资源占比动态调整功能，按需调整密码服务所占虚拟密码机分组资源的比例。 4、应支持密码服务镜像管理，平台级管理员可支持选择特定版本在线升级。 密码资源管理： 1、应支持密码资源动态调整，机构管理员可按需调整、分组密码计算资源（虚拟密码机）、按需调整密码服务实例个数和密码计算资源（虚拟密码机）占比。 2、提供密码设备管理、密码机实例管理、密码服务管理等功能。 3、密码设备管理应支持添加密码设备功能，支持已添加密码设备的详情、编辑、监控、删除等功能。 4、支持查看密码机实例详情信息，如密码机 ID、密码机别名、状态、IP

功能子项	具体要求
	地址、设备主密钥信息、最大连接数、CPU 使用率、内存使用率、连接数等信息。 5、支持对密码计算资源进行分组，实现高可用或者集群化部署，提供连续不间断的密码服务。 6、支持密码计算资源横向扩展和收缩的能力，能够根据业务应用系统的需求进行动态调整。 监控告警： 支持告警功能，可通过邮件、日志系统等多种形式发出；告警内容应包括告警名称、告警级别、告警对象类型、告警时间、告警状态等内容。 日志审计： 1、支持具有日志记录、审计功能，包括系统操作日志、密码服务日志等，提供日志查看及导出功能；日志至少保存 6 个月，并可通过 Syslog、SNMP 进行转发； 2、管理日志审计应提供平台管理日志审计、租户管理日志审计、异常登录日志审计功能。 3、日志审计应支持详情、审核、验签操作功能，审核操作可输入审计说明。 支持数据备份恢复功能。支持用户数据操作日志、审计信息的备份恢复机制；支持平台配置的备份恢复机制。 支持动态扩容，增加系统业务容量，扩容无需停机。
性能要求	支持管理密码机（物理密码机、虚拟密码机）数量≧100 应用数≧100 管理页面操作响应时间< 3 秒 单线程或单进程调用接口服务单笔响应时间<10 毫秒 服务调用并发用户数≧500 个 SM2 签名≧8000 次/秒 SM2 验签≧8000 次/秒 SM4 加解密≧10000 次/秒 SM2 加密≧8000 次/秒 SM2 解密≧8000 次/秒 密钥存储数量≧10 万条 创建对称密钥≧100TPS 创建非对称密钥≧50TPS
安全性要求	1、支持关键程序、文件应实现完整性校验，保证程序运行安全。 2、支持密钥的密文存储，由存储在密码机的主密钥加密保护，保证密钥安全。 3、用户在管理端上的所有操作行为和结果，自动记录并存储。支持日志外发功能，以供查询审计。
稳定性要求	1、支持 7×24 小时稳定运行； 2、密码服务管理模块应具备服务逃生模式。在服务层，当所有密码设备均不可用时，应能通过人工或自动的方式，切换成本地模式，通过软算法完成密码服务运算；在接口层，当所有密码服务均不可用时，应能通过人工或自动的方式，切换成本地模式，通过软算法完成密码接口功能运算； 3、密码服务管理模块应能够正确地执行密码相关的功能和服务，应能够

功能子项	具体要求
	处理各种可能的错误和故障，包括某个服务器故障、某台密码机故障等，确保密码服务的连续性和一致性。
资质要求	产品具备由国家密码管理局商用密码检测中心颁发的《商用密码产品认证证书》，符合 GM/T 0028《密码模块安全技术要求》安全等级第二级要求。

7.2.1.9 配套软件

7.2.1.9.1 服务器版安全操作系统

类别	功能与技术描述
安装环境要求	安全操作系统支持国产主流芯片平台，包括飞腾、鲲鹏、龙芯、兆芯、海光等。
服务器架构要求	安全操作系统支持 X86 和 ARM 架构的服务器，可部署在 X86 和 ARM 架构的服务器环境中。
产品标准符合	拥有自主知识产权的国产操作系统，符合 GB/T29490-2013 知识产权体系管理认证，产品研发过程符合 CMMI4 及以上标准；符合 ISO20000 信息技术服务管理体系标准，提供证书证明材料。
系统功能	具备文件管理、设备管理、日志管理、服务管理、进程和监控管理，网络管理、资源管理、软件包管理、硬盘管理等基本功能，提供语言支持工具、文件共享服务工具、集成开发平台等常用工具。
安装引导	支持 GRUB2 引导，支持 MBR 及 GPT（GUID 分区表）分区，支持 NTFS 文件系统。
文件系统	默认使用 XFS，支持 EXT3、EXT4、GFS、GFS2 等。
常用应用支持	默认提供 apachehttp、ftp、DNS、DHCP、MariaDB、PostgreSQL、NFS、Samba、LDAP 等应用。
存储支持	内置支持快速块设备作为慢速块设备缓存以加速 IO；支持 swap 压缩以减少 IO 并提高性能。
网络协议支持	支持 HTTP、FTP、VNC、TCP、UDP、IP、FTP、DNS、NFS、NTP、DHCP、SSH 等多种网络协议。
系统安全级别管理	系统可提供安全增强组件，支持增加三权分立、白名单控制等安全功能，可增强至国家认证的安全保护级别——结构化保护四级。提供结构化保护四级相关证明材料。
备份还原功能	系统默认提供备份还原工具，支持全盘系统备份、系统增量备份、还原系统等功能。
虚拟化支持	支持 KVM 虚拟化，内置单机虚拟化管理程序，支持作为 Xen、Hyper-V、ESXi 虚拟机。
易用性	提供全中文化的图形操作界面及帮助，采用 i18n（国际化）技术和标准，支持最新国家标准字符集（如：GB18030-2005）
可管理性	提供图形化的远程桌面查看工具，支持 SSH、SPICE、VNC、RDP，协议支持按需启动守护进程。
高可用性	支持负载均衡，支持多种网卡 Bonding，提高可用性。
可维护性	提供在线升级服务，支持动态内核补丁，支持在不重启的情况下为内核打补丁，支持 sosreport 收集系统配置和运行主机上的诊断信息，协

类别	功能与技术描述
	助排查故。
服务	符合 ITSS 信息技术服务标准，提供证明材料。
政府采购需求标准	应满足附件 3《政府采购需求标准》中对应投标产品形态的技术参数要求。

7.2.1.9.2 桌面版安全操作系统

指标项	指标要求
架构支持	支持龙芯、兆芯、飞腾、鲲鹏、海光等主流国产 CPU
产品标准符合	拥有自主知识产权的国产操作系统，符合 GB/T29490-2013 知识产权体系管理认证；符合 ITSS 信息技术服务标准；产品研发过程符合 CMMI5 标准；符合 ISO20000 信息技术服务管理体系标准。须提供证书证明材料
用户界面	提供符合用户使用习惯的图形化人机操作 UI 界面，具有良好的用户操作体验，窗口包括标题栏、菜单栏、状态栏等。
常用应用支持	支持火狐、奇安信浏览器、360 浏览器；提供自研软件，包括视频播放器、文件保护箱、截图软件、刻录软件、语音助手和系统助手，具有图形化粉碎工具；
输入法	支持中文输入法，至少支持搜狗拼音输入法、搜狗五笔输入法、华宇输入法、智能陈桥输入法、王码五笔输入法等。
文件系统支持	支持 Ext3、Ext4、XFS、NTFS 等文件系统。
开发环境支持	支持 Eclipse、Qt 等开发环境； 支持 C/C++、java、php、python、perl 等多种开发语言。
外设支持	支持国内外主流打印机、扫描仪、投影仪、摄像头等各类外设设备。
云打印	对于不提供国产操作系统驱动的打印机型号，可提供云打印方案，支持常规打印参数设置，可查看打印任务状态和日志，可切换不同云端提交任务。
备份还原功能	系统默认提供备份还原工具，支持数据备份、数据还原，支持系统全量备份、系统增量备份，提供一键还原、一键 Ghost 功能。
生物识别	系统提供图形化生物识别管理工具，默认支持指纹、虹膜等多种生物特征识别。图形界面可进行设备驱动开启、关闭及状态查看，默认内置 20 款以上指纹模块驱动。
安全特性	提供安全中心管控工具，提供图形化应用执行控制工具，具有检查应用程序完整性、来源等功能。
账号安全配置	系统提供图形化账号安全配置工具，可支持图形化配置密码复杂度，包括用户名校验、长度、字符、账号锁定配置等。
系统安全级别管理	系统可提供安全增强组件，支持白名单控制等安全功能，可增强至国家认证的安全保护级别，如结构化保护四级。 通过公安部信息安全产品检测中心关于安全操作系统（四级）标准的检测 提供相关证明材料。

指标项	指标要求
支持情况	内置国密算法，支持基于国密算法的加解密应用，支持可信计算。
政府采购需求标准	应满足附件 3《政府采购需求标准》中对应投标产品形态的技术参数要求。

7.2.1.9.3 国密浏览器

指标项	具体要求
兼容性	1、产品及其依赖项满足《GB/T 36572-2018 电力监控系统网络安全防护导则》相关要求，应实现自身的安全，应安全、可控、可靠。 2、产品及其依赖项满足《GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求》3 级。
本体安全	1、产品及其依赖项满足《GB/T 36572-2018 电力监控系统网络安全防护导则》相关要求，应实现自身的安全，应安全、可控、可靠。 2、产品及其依赖项满足《GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求》3 级。
功能要求	实现以下功能的产品及其依赖项，均为本产品的供货范围。 1、支持 SM2、SM3、SM4 等国产密码算法； 2、支持完整的国密通信能力，包括基于 USBKey 的单向、双向认证及 USB Key。 3、配置由第三方权威机构的 CA 根证书，并支持自定义 CA 证书设置； 4、支持浏览器自身安全、环境安全、运行时安全检查，支持插件的安全管控；
资质要求	产品具备由国家密码管理局商用密码检测中心颁发的《商用密码产品认证证书》，符合 GM/T 0028《密码模块安全技术要求》安全等级第二级要求；

7.2.2 安全Ⅱ区、安全接入区

7.2.2.1 总体需求

安全Ⅱ区、安全接入区虚拟化技术平台方案应满足以下几方面的需求：

指标子项	具体要求
统一管理平台要求	设备和资源池纳管：作为统一应用与资源管理的云平台，需要为数据中心的存储设备、网络设备、服务器以及虚拟化技术平台的运行保障提供统一的全栈运维管理能力
	安全管理：为用户提供了用户管理、用户策略管理、认证管理等安全管理功能，帮助用户保证用户信息和系统的安全性。
	监控管理：支持对虚拟化技术平台和各类物理资源进行监控，提取各类资源的监控指标，并支持设定阈值产生相应的阈值告警。
	检查策略：提供检查策略功能，用户可以对系统容量、性能等进行定期检查或手动发起检查，提前发现系统中资源健康风险。
	大屏监控：支持大屏展示功能，提供数据中心概览、性能概览、容量概览预置大屏展示。并提供灵活自定义大屏的能力。

指标子项	具体要求
应用编排	应用的编排是对应用运行时所包含的元素进行管理的描述，包括拓扑描述、部署、弹性伸缩、升级回滚、故障自愈、性能监控等能力。需要结合不同类型的应用提供统一的模型，对应用的全栈进行描述。
应用运维	需要为托管应用的运维人员提供一系列基础及高级运维功能，提供一站式应用运维能力。
自主可控	考虑到系统的可持续性演进，虚拟化技术平台需满足安全自主可控的要求，支持同时纳管 X86 和 ARM 架构的设备，如鲲鹏，飞腾，海光等。
安全可靠	容器平台需保证平台本身的安全性与可靠性，同时应保证管道安全、管理安全、云端数据安全等。
	安全策略管理必须遵从最小授权原则，即不同安全区域内的主机只能访问属于相应区域资源，对数据中心资源必须完全得到控制保护，防止未授权访问

7.2.2.2 基础功能要求

7.2.2.2.1 基础资源管理

指标子项	具体要求
虚拟化支持	支持对于不能容器化的，需要部署在虚拟机上的业务系统的运行支持。
	支持虚拟机镜像运行，原有虚拟机镜像业务系统能运行在容器上。
	统一管理虚拟化应用、容器应用生命周期管理、监控及运维。
	支持虚拟机 HA 高可靠，故障之后自动迁移业务，保障业务高可靠。
	支持对虚拟机一致性快照，当发生故障时保障业务能够快速恢复到快照时间点状态。
	应提供虚拟机镜像、快照完整性校验功能，防止虚拟机镜像被恶意篡改；
	资源调整特性：支持虚拟机在线和离线动态调整，可根据实际需要修改虚拟机的属性，包括 CPU 个数、内存大小、硬盘数量和网卡个数，提升资源利用率。
	动态资源调度：采用智能负载均衡调度算法，周期性检查同一集群资源内各个主机的负载情况，在不同的主机间迁移虚拟机，实现同一集群内不同主机间的负载均衡。
网络管理	随着容器集群规模不断增大，容器数量不断增长，容器网络需能提供更高性能的跨节点通信能力、更大规模的容器网络以及更快的单容器发放性能。同时，容器网络需能够为应用提供各种网络平面、组网模式和节点间的容器网络互通和隔离，如 L2 underlay 组网、L3 overlay 组网等等。
	虚拟机支持网络隔离、安全组等能力保障虚拟机网络安全
	虚拟机支持多 vlan 网络逻辑通信或隔离
存储管理	面向大量有状态应用容器化改造诉求，需要支持容器持久卷。平台需能够支持对接分布式存储或 SAN 存储，支持存储生命周期基本操作（创建、修改、删除、挂载、卸载、回收等）；支持存储容量配置、共享模式设置等。

指标子项	具体要求
镜像/软件包/生命周期管理	平台需提供容器镜像仓库及软件包仓库管理功能，并支持公共仓库和私有仓库两种形式： (1)私有仓库：提供私有镜像或软件包管理功能，其中镜像或软件包只能被有权限用户看到和访问； (2) 公共镜像仓库：提供公共镜像或软件包管理功能，其中镜像或软件包可被系统所有用户都可看到和访问。
镜像仓库	镜像能够提供对应用镜像进行统一管理，包括镜像文件路径、镜像名称、版本、类型等；并提供应用镜像规范的参考模型和流程指导。
	支持私有、公有镜像仓库的创建、更新、查询、删除等（Docker 或 isula 容器镜像包）；
	支持镜像的自动/手动上传下载；
	持镜像私有和公有属性变更；
	支持第三方制品库接入；
	支持自动清理能力。
软件仓库	私有、公有软件仓库的创建、更新、查询、删除等
	支持上传时解压存储，支持存储目录管理。

7.2.2.2.2 应用服务

指标子项	具体要求
应用编排与部署	平台需能够为各种类型的应用（容器应用、虚机应用等）选取合适的资源进行安装部署，并支持运行时管理操作如配置、更新、升级、卸载等。
	提供 Helm 编排；
	提供可视化编排，方便用户以可视化引导方式进行应用组、应用、资源的编排；
	支持单类型应用编排和应用版本混编；
	支持资源编排；
	支持编排服务实例与应用的绑定关系；
	支持无状态应用；
	支持有状态、任务、定时任务的应用部署。
应用调度管理	平台用户需能够指定容器的调度策略，可以为容器运行选择最优节点。具体调度策略应包括：
	应用间的亲和/反亲和性调度：将不同的应用调度部署在相同或不同节点中；
	应用与节点的亲和/反亲和性调度：将应用调度部署到指定的或与指定不同的“操作系统、版本、类型架构”的节点中。
应用弹性伸缩管理	在实际应用中，经常会遇到某个服务需要扩容的场景，也会遇到由于资源紧张或者工作负载降低而需要减少服务实例数量的场景。平台需能够提供多种弹性伸缩的策略。
	自动弹性伸缩模式：组件负载满足预先配置的平台组件自动伸缩策略，根据应用负载程度以及用户配置的伸缩策略，实现应用实例的自

指标子项	具体要求
	动扩缩容，并自动完成负载均衡的调整，过程中需确保业务不中断。
	手动弹性伸缩模式：用户手动确认弹性伸缩的实例数并执行。
应用升级管理	无论是传统的单体应用还是基于外网（综合数据网等）架构的新应用，都无可避免的面临升级问题。平台需能够支持应用滚动升级、替换升级、应用回滚等功能。
	支持应用滚动升级
	按实例个数进行滚动升级；
	按实例个数进行灰度升级；
健康检查与异常恢复	在应用运行过程中应能够根据用户需要定时检查容器健康状况或容器中应用的健康状况，如果检查失败，平台将删除该应用实例，然后根据应用的重启策略来决定是否重启容器。
	平台应提供相应的异常恢复机制，包括但不限于以下情况：
	容器所在节点异常时，容器平台会将其上的容器自动调度到其他的节点；
	容器状态异常时，容器平台自动创建新的容器；
	如故障容器挂载有存储，创建新的容器时自动挂载之前的存储，保证数据不丢失；
	对于有状态应用，新创建的容器名字不改变。

7.2.2.2.3 平台管理

7.2.2.2.3.1 基础资源管理

虚拟化支持双架构部署，可通过一套平台对 x86 和 ARM 架构服务器进行统一管理。

7.2.2.2.3.2 虚拟机、物理机混合管理

平台应以应用为中心，进行统一资源管理和调度，打通物理机、虚拟机、容器等资源，使之互相通信，协同工作。集群中可以添加物理机和 VM 节点，平台提供统一的网络、存储等服务；获取并给用户展示节点详细信息，包括：OS 版本、Docker 版本、CPU、内存、磁盘等，通过统一的管理界面、多维度智能风险预测与智能调优，实现“规划、建设、运维、优化”资源全生命周期自动化管理与智能运维，对多个安全区提供统一管理。

7.2.2.2.3.3 容器平台管理

对应的用户权限管理能力如下：

权限管理，支持创建用户、角色和团队，并能够针对用户、角色或团队，设置不同的资源操作权限。

角色管理，提供界限分明的角色和权限管理功能。

用户认证，支持 LDAP、OAuth2 同步及认证，避免重复创建用户。

用户管理，可以将不同用户设置为不同的角色，方便管理人员对用户的权限划分。

兼容原生的 Kubernetes，通过 kubectl 指令或原生的 api 接口进行编排和管理。通过 UI、kubectl 指令或原生的 api 接口操作时，对子账号控制权限约束一致。

7.2.2.2.3.4 节点和资源管理

可以根据 IP 地址手动添加虚拟机、物理机资源节点；也可以批量导入虚拟机、物理机资源节点；可以通过与 IaaS 对接自动添加虚拟机节点，创建的节点规格可配置，包括 CPU、内存等。

7.2.2.2.3.5 资源池与配额管理

通过容器项目管理，可实现对资源进行逻辑隔离，满足企业内部多个团队的容器资源自服务、自管理。通过为每个应用管理团队划分项目，管理员将团队用户根据权限管理策略完成角色配置，并绑定到项目，以此来实现对用户组资源的逻辑隔离。

提供用户的统一身份认证管理，建立支持基于角色和基于属性的授权检查，并基于配额管理实现应用的准入控制。

支持设置资源池配额，比如可供使用的节点数量、CPU、内存等资源，以及可以创建的容器数量等。配额管理可以针对不同项目设置不同的资源配额（包括 CPU、内存、存储空间、挂载磁盘数量、应用和服务的数量等）

7.2.2.2.3.6 监控、日志、告警管理

平台应提供集群整体运行状态监控。包括进程状态、告警信息等；同时提供对集群节点 CPU 利用率、物理内存利用率、虚拟内存使用率、磁盘使用率等的运行监控。主要包括如下方面：

整个集群的资源占用情况；

每个节点的资源占用情况；

每个节点上的应用实例分布与健康状态；

每个节点上的应用和资源告警汇聚展示。

平台应提供日志服务功能。日志服务需提供可扩展、高可靠和高可用的日志采集、存储、查询和分析功能，能够收集云服务和应用程序生成的日志数据并编制索引，提供实时查询的能力，为分布式服务的故障定界定位提供数据基础，从而保障运维的稳定和高效。日志服务应具备以下特性：

(1) 海量日志采集

可快速收集大规模集群下的日志。通过分布式日志采集、汇聚平台，实现日志实时收集，提高运维效率，保障运维安全。

(2) 统一日志管理

实现日志集中化，提供统一的管理和状态监控，对日志做全文索引，提升搜索效率，并开放 API 接口，对外提供数据接口。

(3) 自定义检索分析

实现日志检索和分析能力，能够自定义查询条件、查询结果，通过用户图形界面来完成强大的搜索、分析功能。

(4) 分布式、可扩展、高可靠和高可用

系统采用高性能、可扩展的分布式架构，支持每日 TB 级别的日志量。同时支持高可靠方案，保证在日志风暴等场景下日志不会丢失。

平台应能够通过灵活的告警策略配置保证监控的快速部署和实施。通过告警策略有效性管理保证告警的准确性，包括对告警的生成策略、告警推送策略进行统一管理。

(1) 告警操作面向监控人员提供告警操作管理功能，包括告警故障定位、告警确认、告警清除、告警通知、告警显示过滤、告警查询等。

(2) 通过告警提醒能够实现对平台运行异常状况的及时处理，保障平台运行的稳定性。告警提醒为平台提供告警生成、告警自动处理等灵活的策略配置功能。根据平台的物理资源、逻辑资源、应用资源的运行状态生成告警数据

7.2.2.2.3.7 集群部署运维

支持容器云平台管控组件，和容器云平台的业务应用，分别部署在不同的 k8s 集群上，实现控制链路与业务数据链路的隔离。

支持应用的多集群统一管理，集群部署升级需要有良好的体验。

支持在线业务系统和离线业务系统混合部署能力。

7.2.2.3 中间件服务

7.2.2.3.1 企业级分布式应用服务（微服务）

企业级分布式应用服务是分布式架构和数字化业务上云的应用托管平台，典型应用场景包括容器应用、虚拟机应用等。

支持运维人员快捷进行集群维护；支持应用的生命周期管理，应用版本管理、部署、升级、健康检查等能力，极大提升运维管理效率。

应用版本管理：支持应用版本的配置、上传、下载等操作，支持通过多个应用版本管理适配不同架构类型、不同参数配置的不同类型应用。

应用部署：支持根据需要及应用版本配置部署多个应用，支持查看应用的运行状态。

应用升级：支持对已部署的应用进行升级。

健康检查：支持定时探测容器/进程的健康状况，在健康检查不正常时自动重启模块实例。

7.2.2.3.2 分布式消息队列

基于 Kafka 的分布式消息队列，支持消息的持久化存储和批量处理，能够有效地处理大规模的数据流。

不同系统和应用程序可以通过分布式消息队列进行实时的数据交换和消息传递，从而实现系统之间的解耦和数据的实时同步。在海量消息堆积的情况下，始终能保持消息队列的高吞吐能力。

7.2.2.3.3 内存数据库

内存数据库是兼容 Redis 协议标准的数据库服务，基于双机热备架构及集群架构，可满足高吞吐、低延迟及弹性变配等业务需求。集群兼容性高，支持 string，hash，list，set，sortedset 等常见类型，支持事务和订阅。提供多种规格的缓存数据库实例，支持实例的创建、重启、释放、备份等管理操作，支持清除全部数据和清理过期数据；支持实例的网络隔离。

内存数据库支持多样化存储的场景：存储数据库使用；缓存加速应用访问。

7.2.2.4 安全服务

整体要求：根据《GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求》第 3 级安全要求，满足安全通用要求和云计算扩展要求，进行定级、防护、测评及备案。应满足《GB/T 25070-2019 信息安全技术网络安全等级保护安全设计技术要求》第 3 级系统安全设计要求。产品应为安全自主可控产品（包括芯片和操作系统等）。安全软硬件资源的授权需为永久授权，且病毒库、特征库等具备时效性的数据库需同时提供十年的免费离线更新服务。

7.2.2.4.1 主机安全

功能子项	具体要求
兼容性	1、产品及其依赖项满足《GB/T 36572-2018 电力监控系统网络安全防护导

	则》相关要求，应实现自身的安全，应安全、可控、可靠。 2、产品及其依赖项满足《GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求》3 级。
本体安全	1、产品及其依赖项满足《GB/T 36572-2018 电力监控系统网络安全防护导则》相关要求，应实现自身的安全，应安全、可控、可靠。 2、产品及其依赖项满足《GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求》3 级。 3、可限制仅特定地址登录。 4、远程管理设备时，应建立安全的通信协议。
授权要求	支持≧1500 个 IP
功能要求	实现以下功能的产品及其依赖项，均为本产品的供货范围： 1．支持病毒查杀，支持开启或停用。 2．支持展示重点关注的资产、漏洞、异常、配置缺陷、事件等信息。 3．支持进行资产暴露盘点，可提供资产、暴露组件、暴露端口、可被利用的漏洞、暴露风险详情、暴露中间件名称、类型、版本、关联漏洞、影响资产、最新扫描时间等信息。 4．支持对云服务器进行最佳实践基线检查，发现操作系统和应用软件的配置弱项。 5．支持弱口令基线检查，包括检测弱口令账号等。 6．支持漏洞管理，包括 linux 系统漏洞、web 应用漏洞、弱口令漏洞等。 7．支持等保合规等保二、三级标准检查。 8．支持登录日志、暴力破解、安全基线、入侵防御事件等日志查询。 9．支持中间件类型、主机的计划任务、主机端口监听信息、主机账户信息、主机软件安装的资产信息、主机进程信息、启动项数据等资产管理。 10．支持病毒库的集中管控及分发。定期对服务器端病毒库更新，保持病毒库处于最新状态，集中统一下发管控的节点进行病毒查杀。

7.2.2.4.2 蜜罐系统

蜜罐基于伪装欺骗技术，通过在攻击者入侵的关键路径上部署诱饵和陷阱，诱导攻击者进入与真实网络隔离的蜜网，让攻击者在蜜网中攻击伪装的服务、获取虚假的数据，进而完整记录攻击者行为，捕获高级未知攻击，并且对攻击者做取证和追踪溯源，为防守方提供先人一步的主动防御手段，保护真实资产，提升主动防御的能力。

功能子项	具体要求
兼容性	产品兼容市场主流厂家虚拟化技术平台部署
伪装诱捕	支持 Web 类蜜罐，包括但不限于 Thinkphp6、Jenkins、Zabbix、Webmin、Struts2、Web 自定义蜜罐等。
	支持中间件类蜜罐，包括但不限于 Tomcat、Weblogic、JBoss 等。
	支持数据库类蜜罐，包括但不限于 MySQL、PostgreSQL 、MongoDB、Redis 等。
	支持系统服务类蜜罐，包括但不限于 RDP、DNS、SSH、FTP、Telnet、

功能子项	具体要求
	VPN 等。
	支持在线制作感知型文件蜜饵，支持格式种类包括但不限于 doc、xls、ppt、pdf 等，部署在业务系统上或散布于公网中，一旦攻击者触碰蜜饵，系统将产生相应告警。
	支持在线克隆和导入克隆包两种方式，一键应用于蜜罐节点，实现统一管理，提升蜜罐甜度，加强诱捕能力。
	支持查看蜜罐节点的资源使用情况，并对蜜罐节点的管理，如暂停、停止、重启、快照、删除等操作。
	提供高灵活度的自定义拓扑能力，支持用户自由拖动内置组件构建真实网络架构，在态势感知大屏中进行个性化展示。
攻击分析	支持基于攻击事件聚合攻击行为，捕获某一攻击者对某一蜜罐/蜜饵产生的所有攻击，并按照时间轴形式详细展示攻击过程。
	支持攻击者指纹溯源，获取攻击者硬件指纹和系统指纹信息，包括但不限于：显卡/声卡/屏幕分辨率/MAC 地址/CPU 核心数/操作系统类型/版本/系统语言/时区等。
	支持攻击者社交账号溯源，支持多种主流社交平台账号信息（包括用户 ID/用户昵称/用户头像等）。
	支持生成、预览、导出欺骗诱捕系统攻击报告，导出格式为 PDF、WORD 等。
系统管理	支持系统三权分立管理模式：系统管理员、操作员、审计员相互独立，不同账户拥有不同业务功能模块管理权限。
	支持多因子认证，提供多种登录认证方式。

7.2.2.5 商用密码服务

整体要求：按照《GB/T 39786-2021 信息安全技术信息系统密码应用基本要求》三级要求，实现密码应用。产品应为安全自主可控产品，满足国产商用密码技术，达到《GB/T 37092 信息安全技术 密码模块安全要求》二级及以上安全要求。

7.2.2.5.1 密码服务管理平台

功能子项	具体要求
兼容性	1、产品及其依赖项满足《GB/T 36572-2018 电力监控系统网络安全防护导则》相关要求，应实现自身的安全，应安全、可控、可靠。 2、产品及其依赖项满足《GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求》3 级。
本体安全	1、产品及其依赖项满足《GB/T 36572-2018 电力监控系统网络安全防护导则》相关要求，应实现自身的安全，应安全、可控、可靠。 2、产品及其依赖项满足《GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求》3 级。 3、可限制仅特定地址登录；

功能子项	具体要求
	4、远程管理设备时，应建立安全的通信协议； 5、支持国密双因子身份鉴别、应配置复杂口令并开启定期强制改密，配置国密 Ukey 数≧3；
服务调度	1、支持对服务器密码机等密码设备密码资源统一调度，为上层系统及应用提供按需高效、弹性可扩展的密码服务； 2、支持提供密码服务的基础管控能力，包括密码运算资源映射管理、密码资源弹性分配、密码资源灵活控制等功能； 3、支持资源动态分配，利用负载均衡技术实现虚拟化实例对密码资源占用的动态分配； 4、支持向业务或平台应用提供统一丰富的密码功能接口，满足各种场景下的密码应用需求。
数据加解密	1、支持基于国产商密算法、国际密码算法的对称加解密、非对称加解密等服务功能。 2、支持重要数据（鉴别数据、重要业务数据、日志数据、访问控制信息）加解密功能。 3、支持数据库加解密服务功能，可应用于国产数据库。 4、支持对称算法的传输数据或文件加密、解密服务，支持使用公钥加密会话密钥、会话密钥加密数据的方式对传输数据或文件进行加密。 5、支持基于对称算法对结构化数据或文件的安全存储进行加密和解密。 6、支持对称密钥、非对称密钥的申请服务，申请对称密钥时，支持公钥加密输出密文或采用数字信封的方式加密输出。
签名验签	1、支持可信根证书管理，可同时采信多个厂商 CA 根证书。 2、可同时配置多条证书链，验证不同 CA 系统签发的数字证书。 3、提供证书解析功能， 获取证书中的任意主题信息以及扩展项信息。 4、实现基于数字证书的身份认证，支持不同 CA 的证书验证，提供 CRL/OCSP 等多种方式的证书有效性验证。 5、支持 PKCS#1、PKCS#7 Attach、PKCS#7 Dettach、PKCS#7 数字信封、XML 等标准格式的数字签名。 6、支持对文件的数字签名和数字签名验证功能。
密钥管理	1、支持对密钥的全生命周期管理功能，支持密钥的生成、存储、备份、恢复、销毁、归档等功能。 2、支持 SM1、SM2、SM3、SM4、SM7、SM9 等国产密码算法。 3、提供创建外部密钥功能，支持将用户自有密钥加密导入密钥管理服务。 4、支持通过密钥版本化和定期轮转来加强密钥使用的安全性，提供应用完全透明的密钥自动轮转能力。 5、支持应用管理，支持密钥授权给指定应用。
平台管理	系统管理： 1、系统管理应提供用户管理、角色管理、授权管理、系统日志等管理功能。 2、用户管理应支持用户的添加、编辑、USB Key 绑定、重置口令、删除等操作。 3、角色管理支持角色的添加、编辑、删除等操作。 4、系统日志应支持日志的查看与下载。 资源总览：

功能子项	具体要求
	1、提供统一的管理入口，统一管理密码服务资源和密码计算资源。 2、支持对密码服务管理平台、密码资源的运行情况监控，包含密码资源使用状态、业务资源使用状态和运行状态； 3、应支持密码资源态势监控，平台级管理员可监控对象应包括：密码服务调用概况和调用历史、密码计算资源运行概况、密码服务资源运行概况、密码服务分类分布概况和调用分布概况，支持 Web 大屏方式展示。 4、应支持密码服务资源监控，监控类型分为资源监控和业务监控，资源监控指标应包括：密码服务实例的处理器、内存、网络流量；业务监控指标应包括：密码服务整体和类别的 TPS、平均响应值。支持按时间区间统计实时和历史监控数据的能力。 密码服务管理： 1、密码服务管理支持服务的详情查看和监控操作。 2、支持密码服务实例的配置、监控、升级、重启、关闭、释放、备份和恢复的功能。 3、支持密码服务资源占比动态调整功能，按需调整密码服务所占虚拟密码机分组资源的比例。 4、应支持密码服务镜像管理，平台级管理员可支持选择特定版本在线升级。 密码资源管理： 1、应支持密码资源动态调整，机构管理员可按需调整、分组密码计算资源（虚拟密码机）、按需调整密码服务实例个数和密码计算资源（虚拟密码机）占比。 2、提供密码设备管理、密码机实例管理、密码服务管理等功能。 3、密码设备管理应支持添加密码设备功能，支持已添加密码设备的详情、编辑、监控、删除等功能。 4、支持查看密码机实例详情信息，如密码机 ID、密码机别名、状态、IP 地址、设备主密钥信息、最大连接数、CPU 使用率、内存使用率、连接数等信息。 5、支持对密码计算资源进行分组，实现高可用或者集群化部署，提供连续不间断的密码服务。 6、支持密码计算资源横向扩展和收缩的能力，能够根据业务应用系统的需求进行动态调整。 监控告警： 支持告警功能，可通过邮件、日志系统等多种形式发出；告警内容应包括告警名称、告警级别、告警对象类型、告警时间、告警状态等内容。 日志审计： 1、支持具有日志记录、审计功能，包括系统操作日志、密码服务日志等，提供日志查看及导出功能；日志至少保存 6 个月，并可通过 Syslog、SNMP 进行转发； 2、管理日志审计应提供平台管理日志审计、租户管理日志审计、异常登录日志审计功能。 3、日志审计应支持详情、审核、验签操作功能，审核操作可输入审计说明。 支持数据备份恢复功能。支持用户数据操作日志、审计信息的备份恢复

功能子项	具体要求
	机制；支持平台配置的备份恢复机制。 支持动态扩容，增加系统业务容量，扩容无需停机。
性能要求	支持管理密码机（物理密码机、虚拟密码机）数量≧100 应用数≧100 管理页面操作响应时间< 3 秒 单线程或单进程调用接口服务单笔响应时间<10 毫秒 服务调用并发用户数≧500 个 SM2 签名≧8000 次/秒 SM2 验签≧8000 次/秒 SM4 加解密≧10000 次/秒 SM2 加密≧8000 次/秒 SM2 解密≧8000 次/秒 密钥存储数量≧10 万条 创建对称密钥≧100TPS 创建非对称密钥≧50TPS
安全性要求	1、支持关键程序、文件应实现完整性校验，保证程序运行安全。 2、支持密钥的密文存储，由存储在密码机的主密钥加密保护，保证密钥安全。 3、用户在管理端上的所有操作行为和结果，自动记录并存储。支持日志外发功能，以供查询审计。
稳定性要求	1、支持 7×24 小时稳定运行； 2、密码服务管理模块应具备服务逃生模式。在服务层，当所有密码设备均不可用时，应能通过人工或自动的方式，切换成本地模式，通过软算法完成密码服务运算；在接口层，当所有密码服务均不可用时，应能通过人工或自动的方式，切换成本地模式，通过软算法完成密码接口功能运算； 3、密码服务管理模块应能够正确地执行密码相关的功能和服务，应能够处理各种可能的错误和故障，包括某个服务器故障、某台密码机故障等，确保密码服务的连续性和一致性。
资质要求	产品具备由国家密码管理局商用密码检测中心颁发的《商用密码产品认证证书》，符合 GM/T 0028《密码模块安全技术要求》安全等级第二级要求。

7.2.2.6 配套软件

7.2.2.6.1 服务器版安全操作系统

类别	功能与技术描述
安装环境要求	安全操作系统支持国产主流芯片平台，包括飞腾、鲲鹏、龙芯、兆芯、海光等。
服务器架构要求	安全操作系统支持 X86 和 ARM 架构的服务器，可部署在 X86 和 ARM 架构的服务器环境中。
产品标准符合	拥有自主知识产权的国产操作系统，符合 GB/T29490-2013 知识产权体

类别	功能与技术描述
	系管理认证，产品研发过程符合 CMMI4 及以上标准；符合 ISO20000 信息技术服务管理体系标准，提供证书证明材料。
系统功能	具备文件管理、设备管理、日志管理、服务管理、进程和监控管理，网络管理、资源管理、软件包管理、硬盘管理等基本功能，提供语言支持工具、文件共享服务工具、集成开发平台等常用工具。
安装引导	支持 GRUB2 引导，支持 MBR 及 GPT（GUID 分区表）分区，支持 NTFS 文件系统。
文件系统	默认使用 XFS，支持 EXT3、EXT4、GFS、GFS2 等。
常用应用支持	默认提供 apachehttp、ftp、DNS、DHCP、MariaDB、PostgreSQL、NFS、Samba、LDAP 等应用。
存储支持	内置支持快速块设备作为慢速块设备缓存以加速 IO；支持 swap 压缩以减少 IO 并提高性能。
网络协议支持	支持 HTTP、FTP、VNC、TCP、UDP、IP、FTP、DNS、NFS、NTP、DHCP、SSH 等多种网络协议。
系统安全级别管理	系统可提供安全增强组件，支持增加三权分立、白名单控制等安全功能，可增强至国家认证的安全保护级别——结构化保护四级。提供结构化保护四级相关证明材料。
备份还原功能	系统默认提供备份还原工具，支持全盘系统备份、系统增量备份、还原系统等功能。
虚拟化支持	支持 KVM 虚拟化，内置单机虚拟化管理程序，支持作为 Xen、Hyper-V、ESXi 虚拟机。
易用性	提供全中文化的图形操作界面及帮助，采用 i18n（国际化）技术和标准，支持最新国家标准字符集（如：GB18030-2005）.
可管理性	提供图形化的远程桌面查看工具，支持 SSH、SPICE、VNC、RDP，协议支持按需启动守护进程。
高可用性	支持负载均衡，支持多种网卡 Bonding，提高可用性。
可维护性	提供在线升级服务，支持动态内核补丁，支持在不重启的情况下为内核打补丁，支持 sosreport 收集系统配置和运行主机上的诊断信息，协助排查故。
服务	符合 ITSS 信息技术服务标准，提供证明材料。
政府采购需求标准	应满足附件 3《政府采购需求标准》中对应投标产品形态的技术参数要求。

7.2.2.6.2 国密浏览器

指标项	具体要求
兼容性	1、产品及其依赖项满足《GB/T 36572-2018 电力监控系统网络安全防护导则》相关要求，应实现自身的安全，应安全、可控、可靠。 2、产品及其依赖项满足《GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求》3 级。
本体安全	1、产品及其依赖项满足《GB/T 36572-2018 电力监控系统网络安全防护导则》相关要求，应实现自身的安全，应安全、可控、可靠。 2、产品及其依赖项满足《GB/T 22239-2019 信息安全技术 网络安全等级

指标项	具体要求
	保护基本要求》3 级。
功能要求	实现以下功能的产品及其依赖项，均为本产品的供货范围： 1、支持 SM2、SM3、SM4 等国产密码算法。 2、支持完整的国密通信能力，包括基于 USBKey 的单向、双向认证及 USB Key。 3、配置由第三方权威机构的 CA 根证书，并支持自定义 CA 证书设置。 4、支持浏览器自身安全、环境安全、运行时安全检查，支持插件的安全管控。
资质要求	产品具备由国家密码管理局商用密码检测中心颁发的《商用密码产品认证证书》，符合 GM/T 0028《密码模块安全技术要求》安全等级第二级要求。

7.2.3 安全Ⅰ区

7.2.3.1 安全服务

7.2.3.1.1 主机安全

功能子项	具体要求
兼容性	1、产品及其依赖项满足《GB/T 36572-2018 电力监控系统网络安全防护导则》相关要求，应实现自身的安全，应安全、可控、可靠。 2、产品及其依赖项满足《GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求》3 级。
本体安全	1、产品及其依赖项满足《GB/T 36572-2018 电力监控系统网络安全防护导则》相关要求，应实现自身的安全，应安全、可控、可靠。 2、产品及其依赖项满足《GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求》3 级。 3、可限制仅特定地址登录。 4、远程管理设备时，应建立安全的通信协议。
授权要求	支持≧1500 个 IP
功能要求	实现以下功能的产品及其依赖项，均为本产品的供货范围： 1. 支持病毒查杀，支持开启或停用。 2. 支持展示重点关注的资产、漏洞、异常、配置缺陷、事件等信息。 3. 支持进行资产暴露盘点，可提供资产、暴露组件、暴露端口、可被利用的漏洞、暴露风险详情、暴露中间件名称、类型、版本、关联漏洞、影响资产、最新扫描时间等信息。 4. 支持对云服务器进行最佳实践基线检查，发现操作系统和应用软件的配置弱项。 5. 支持弱口令基线检查，包括检测弱口令账号等。 6. 支持漏洞管理，包括 linux 系统漏洞、web 应用漏洞、弱口令漏洞等。 7. 支持等保合规等保二、三级标准检查。 8. 支持登录日志、暴力破解、安全基线、入侵防御事件等日志查询。 9. 支持中间件类型、主机的计划任务、主机端口监听信息、主机账户信息、主机软件安装的资产信息、主机进程信息、启动项数据等资产管理。

	10. 支持病毒库的集中管控及分发。定期对服务器端病毒库更新，保持病毒库处于最新状态，集中统一下发管控的节点进行病毒查杀。

7.2.3.2 商用密码服务

7.2.3.2.1 密码服务管理平台

功能子项	具体要求
兼容性	1、产品及其依赖项满足《GB/T 36572-2018 电力监控系统网络安全防护导则》相关要求，应实现自身的安全，应安全、可控、可靠。 2、产品及其依赖项满足《GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求》3 级。
本体安全	1、产品及其依赖项满足《GB/T 36572-2018 电力监控系统网络安全防护导则》相关要求，应实现自身的安全，应安全、可控、可靠。 2、产品及其依赖项满足《GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求》3 级。 3、可限制仅特定地址登录； 4、远程管理设备时，应建立安全的通信协议； 5、支持国密双因子身份鉴别、应配置复杂口令并开启定期强制改密，配置国密 Ukey 数≧3；
服务调度	1、支持对服务器密码机等密码设备密码资源统一调度，为上层系统及应用提供按需高效、弹性可扩展的密码服务； 2、支持提供密码服务的基础管控能力，包括密码运算资源映射管理、密码资源弹性分配、密码资源灵活控制等功能； 3、支持资源动态分配，利用负载均衡技术实现虚拟化实例对密码资源占用的动态分配； 4、支持向业务或平台应用提供统一丰富的密码功能接口，满足各种场景下的密码应用需求。
数据加解密	1、支持基于国产商密算法、国际密码算法的对称加解密、非对称加解密等服务功能。 2、支持重要数据（鉴别数据、重要业务数据、日志数据、访问控制信息）加解密功能。 3、支持数据库加解密服务功能，可应用于国产数据库。 4、支持对称算法的传输数据或文件加密、解密服务，支持使用公钥加密会话密钥、会话密钥加密数据的方式对传输数据或文件进行加密。 5、支持基于对称算法对结构化数据或文件的安全存储进行加密和解密。 6、支持对称密钥、非对称密钥的申请服务，申请对称密钥时，支持公钥加密输出密文或采用数字信封的方式加密输出。
签名验签	1、支持可信根证书管理，可同时采信多个厂商 CA 根证书。 2、可同时配置多条证书链，验证不同 CA 系统签发的数字证书。 3、提供证书解析功能， 获取证书中的任意主题信息以及扩展项信息。 4、实现基于数字证书的身份认证，支持不同 CA 的证书验证，提供 CRL/OCSP 等多种方式的证书有效性验证。 5、支持 PKCS#1、PKCS#7 Attach、PKCS#7 Dettach、PKCS#7 数字信封、

功能子项	具体要求
	XML 等标准格式的数字签名。 6、支持对文件的数字签名和数字签名验证功能。
密钥管理	1、支持对密钥的全生命周期管理功能，支持密钥的生成、存储、备份、恢复、销毁、归档等功能。 2、支持 SM1、SM2、SM3、SM4、SM7、SM9 等国产密码算法。 3、提供创建外部密钥功能，支持将用户自有密钥加密导入密钥管理服务。 4、支持通过密钥版本化和定期轮转来加强密钥使用的安全性，提供应用完全透明的密钥自动轮转能力。 5、支持应用管理，支持密钥授权给指定应用。
平台管理	系统管理： 1、系统管理应提供用户管理、角色管理、授权管理、系统日志等管理功能。 2、用户管理应支持用户的添加、编辑、USB Key 绑定、重置口令、删除等操作。 3、角色管理支持角色的添加、编辑、删除等操作。 4、系统日志应支持日志的查看与下载。 资源总览： 1、提供统一的管理入口，统一管理密码服务资源和密码计算资源。 2、支持对密码服务管理平台、密码资源的运行情况监控，包含密码资源使用状态、业务资源使用状态和运行状态； 3、应支持密码资源态势监控，平台级管理员可监控对象应包括：密码服务调用概况和调用历史、密码计算资源运行概况、密码服务资源运行概况、密码服务分类分布概况和调用分布概况，支持 Web 大屏方式展示。 4、应支持密码服务资源监控，监控类型分为资源监控和业务监控，资源监控指标应包括：密码服务实例的处理器、内存、网络流量；业务监控指标应包括：密码服务整体和类别的 TPS、平均响应值。支持按时间区间统计实时和历史监控数据的能力。 密码服务管理： 1、密码服务管理支持服务的详情查看和监控操作。 2、支持密码服务实例的配置、监控、升级、重启、关闭、释放、备份和恢复的功能。 3、支持密码服务资源占比动态调整功能，按需调整密码服务所占虚拟密码机分组资源的比例。 4、应支持密码服务镜像管理，平台级管理员可支持选择特定版本在线升级。 密码资源管理： 1、应支持密码资源动态调整，机构管理员可按需调整、分组密码计算资源（虚拟密码机）、按需调整密码服务实例个数和密码计算资源（虚拟密码机）占比。 2、提供密码设备管理、密码机实例管理、密码服务管理等功能。 3、密码设备管理应支持添加密码设备功能，支持已添加密码设备的详情、编辑、监控、删除等功能。 4、支持查看密码机实例详情信息，如密码机 ID、密码机别名、状态、IP 地址、设备主密钥信息、最大连接数、CPU 使用率、内存使用率、连接

功能子项	具体要求
	数等信息。 5、支持对密码计算资源进行分组，实现高可用或者集群化部署，提供连续不间断的密码服务。 6、支持密码计算资源横向扩展和收缩的能力，能够根据业务应用系统的需求进行动态调整。 监控告警： 支持告警功能，可通过邮件、日志系统等多种形式发出；告警内容应包括告警名称、告警级别、告警对象类型、告警时间、告警状态等内容。 日志审计： 1、支持具有日志记录、审计功能，包括系统操作日志、密码服务日志等，提供日志查看及导出功能;日志至少保存 6 个月，并可通过 Syslog、SNMP 进行转发； 2、管理日志审计应提供平台管理日志审计、租户管理日志审计、异常登录日志审计功能。 3、日志审计应支持详情、审核、验签操作功能，审核操作可输入审计说明。 支持数据备份恢复功能。支持用户数据操作日志、审计信息的备份恢复机制；支持平台配置的备份恢复机制。 支持动态扩容，增加系统业务容量，扩容无需停机。
性能要求	支持管理密码机（物理密码机、虚拟密码机）数量≧100 应用数≧100 管理页面操作响应时间< 3 秒 单线程或单进程调用接口服务单笔响应时间<10 毫秒 服务调用并发用户数≧500 个 SM2 签名≧8000 次/秒 SM2 验签≧8000 次/秒 SM4 加解密≧10000 次/秒 SM2 加密≧8000 次/秒 SM2 解密≧8000 次/秒 密钥存储数量≧10 万条 创建对称密钥≧100TPS 创建非对称密钥≧50TPS
安全性要求	1、支持关键程序、文件应实现完整性校验，保证程序运行安全。 2、支持密钥的密文存储，由存储在密码机的主密钥加密保护，保证密钥安全。 3、用户在管理端上的所有操作行为和结果，自动记录并存储。支持日志外发功能，以供查询审计。
稳定性要求	1、支持 7×24 小时稳定运行； 2、密码服务管理模块应具备服务逃生模式。在服务层，当所有密码设备均不可用时，应能通过人工或自动的方式，切换成本地模式，通过软算法完成密码服务运算；在接口层，当所有密码服务均不可用时，应能通过人工或自动的方式，切换成本地模式，通过软算法完成密码接口功能运算； 3、密码服务管理模块应能够正确地执行密码相关的功能和服务，应能够

功能子项	具体要求
	处理各种可能的错误和故障，包括某个服务器故障、某台密码机故障等，确保密码服务的连续性和一致性。
资质要求	产品具备由国家密码管理局商用密码检测中心颁发的《商用密码产品认证证书》，符合 GM/T 0028《密码模块安全技术要求》安全等级第二级要求。

7.2.3.3 配套软件

7.2.3.3.1 服务器版安全操作系统

类别	功能与技术描述
安装环境要求	安全操作系统支持国产主流芯片平台，包括飞腾、鲲鹏、龙芯、兆芯、海光等。
服务器架构要求	安全操作系统支持 X86 和 ARM 架构的服务器，可部署在 X86 和 ARM 架构的服务器环境中。
产品标准符合	拥有自主知识产权的国产操作系统，符合 GB/T29490-2013 知识产权体系管理认证，产品研发过程符合 CMMI4 及以上标准；符合 ISO20000 信息技术服务管理体系标准，提供证书证明材料。
系统功能	具备文件管理、设备管理、日志管理、服务管理、进程和监控管理，网络管理、资源管理、软件包管理、硬盘管理等基本功能，提供语言支持工具、文件共享服务工具、集成开发平台等常用工具。
安装引导	支持 GRUB2 引导，支持 MBR 及 GPT（GUID 分区表）分区，支持 NTFS 文件系统。
文件系统	默认使用 XFS，支持 EXT3、EXT4、GFS、GFS2 等。
常用应用支持	默认提供 apachehttp、ftp、DNS、DHCP、MariaDB、PostgreSQL、NFS、Samba、LDAP 等应用。
存储支持	内置支持快速块设备作为慢速块设备缓存以加速 IO；支持 swap 压缩以减少 IO 并提高性能。
网络协议支持	支持 HTTP、FTP、VNC、TCP、UDP、IP、FTP、DNS、NFS、NTP、DHCP、SSH 等多种网络协议。
系统安全级别管理	系统可提供安全增强组件，支持增加三权分立、白名单控制等安全功能，可增强至国家认证的安全保护级别——结构化保护四级。提供结构化保护四级相关证明材料。
备份还原功能	系统默认提供备份还原工具，支持全盘系统备份、系统增量备份、还原系统等功能。
虚拟化支持	支持 KVM 虚拟化，内置单机虚拟化管理程序，支持作为 Xen、Hyper-V、ESXi 虚拟机。
易用性	提供全中文化的图形操作界面及帮助，采用 i18n（国际化）技术和标准，支持最新国家标准字符集（如：GB18030-2005）.
可管理性	提供图形化的远程桌面查看工具，支持 SSH、SPICE、VNC、RDP，协议支持按需启动守护进程。
高可用性	支持负载均衡，支持多种网卡 Bonding，提高可用性。

类别	功能与技术描述
可维护性	提供在线升级服务，支持动态内核补丁，支持在不重启的情况下为内核打补丁，支持 sosreport 收集系统配置和运行主机上的诊断信息，协助排查故。
服务	符合 ITSS 信息技术服务标准，提供证明材料。
政府采购需求标准	应满足附件 3《政府采购需求标准》中对应投标产品形态的技术参数要求。

7.2.4 监测信息跨安全区传输

边缘集群各个安全区域平台监测信息，需要通过物理隔离装置实现监测信息跨安全区传输，最终全部汇总在贵州计量检定中心基地的安全III区的平台中，并在安全III区的平台中进行信息的统一展现和监测，由各个安全区域的实施单位负责把信息传输至安全III区，并配合贵州计量检定中心基地安全III区的平台厂家实现数据的接入和展现。贵州计量检定基地安全III区平台收到各个安全区域的监测信息后负责采用云边协同规范，把监测信息上送至调度云棠下延伸节点（数据分析域）。

7.2.5 综合监管系统

在贵州计量自动化系统 3.0 安全接入区部署安全接入区态势感知中继系统、安全Ⅱ区部署态势感知子站系统、安全III区部署态势感知子站系统，包括集成部署及接口联调等内容。

7.2.5.1 安全接入区态势感知中继系统

在贵州计量自动化系统 3.0 安全接入区部署安全接入区态势感知中继系统，本系统负责将接入区态势感知探针采集信息跨隔离推送到安全Ⅱ区部署的态势感知子站系统。安全接入区态势感知中继系统具备控制通道代理、报文通道代理、代理模块数据处理等功能，提供数据报文解析、封装、代理转发等服务，实现隔离装置的数据穿透、以及厂级采集数据、主站控制指令的数据转发代理。

7.2.5.2 安全Ⅱ区态势感知子站系统

在贵州计量自动化系统 3.0 安全Ⅱ区部署态势感知子站系统（本系统能够识别来自安全接入区、安全Ⅰ区、Ⅱ区的态势感知探针推送的日志，实现端口诱捕以及子站系统所有接入设备的范式化解析，识别分析 102 规约流量等，并能实现相关界面展示），计量 3.0 部署的安全Ⅱ区态势感知子站系统能将处理分析后的数据传送到调度的安全Ⅱ区态势感知主站系统。

本态势感知子站系统还应具备以下功能：

实时监测：

实时监视从自身脆弱性、外部威胁和安全指数等三个方面，实时反映了区域内贵州计量自动化系统 3.0 的网络安全态势。

自身脆弱性监视指贵州计量自动化系统 3.0 资产及其防护措施的安全状态及合规程度，包括资产发现、互联拓扑、运行状态、开放服务、配置合规和系统漏洞等方面的监视。外部威胁监视是指贵州计量自动化系统 3.0 的资产可能受到来自外部安全侵害的可能及影响，包括网络行为、外设接入、登录操作和程序代码等内容的监视。安全指数描述系统网络安全的整体态势。

历史审计：

历史审计通过对脆弱性、威胁度相关历史数据的统计和分析，反映了区域内贵州计量自动化系统 3.0 的历史网络安全态势。

数据处理：

本系统以设备资产为基础，建立贵州计量自动化系统 3.0 的网络安全模型，贵州计量自动化系统 3.0 的网络安全模型分为外部威胁和自身脆弱性两方面。其中，外部威胁包括网络行为信息、移动介质接入信息、代码程序信息和人为登录操作信息；内部脆弱性包括资产信息、拓扑连接信息、运行状态信息、开放服务信息、配置合规信息、系统漏洞信息。

本系统具备告警管理功能，告警包括站点名称、设备类型、设备名称、告警类型、告警等级、告警内容、告警详情、告警开始时间、最新告警时间、重复次数。

7.2.5.3 安全III区态势感知子站系统

在贵州计量自动化系统 3.0 安全III区部署态势感知子站系统（本系统能够识别来自安全III区的态势感知探针推送的日志，实现端口诱捕以及子站系统所有接入设备的范式化解析等，并能实现相关界面展示），计量 3.0 部署的安全III区态势感知子站系统能将处理分析后的数据传送到调度的安全III区态势感知主站系统。

本态势感知子站系统还应具备以下功能：

实时监测：

实时监视从自身脆弱性、外部威胁和安全指数等三个方面，实时反映了区域内贵州计量自动化系统 3.0 的网络安全态势。

自身脆弱性监视指贵州计量自动化系统 3.0 资产及其防护措施的安全状态及合规程度，包括资产发现、互联拓扑、运行状态、开放服务、配置合规和系统漏洞等方面的监视。外部威胁监视是指贵州计量自动化系统 3.0 的资产可能受到来自外部安全侵害的可能及影响，包括网络行为、外设接入、登录操作和程序代码等内容的监视。安全指数描述系统网络安全的整体态势。

历史审计：

历史审计通过对脆弱性、威胁度相关历史数据的统计和分析，反映了区域内贵州计量自动化系统 3.0 的历史网络安全态势。

数据处理：

本系统以设备资产为基础，建立贵州计量自动化系统 3.0 的网络安全模型，贵州计量自动化系统 3.0 的网络安全模型分为外部威胁和自身脆弱性两方面。其中，外部威胁包括网络行为信息、移动介质接入信息、代码程序信息和人为登录操作信息；内部脆弱性包括资产信息、拓扑连接信息、运行状态信息、开放服务信息、配置合规信息、系统漏洞信息。

本系统具备告警管理功能，告警包括站点名称、设备类型、设备名称、告警类型、告警等级、告警内容、告警详情、告警开始时间、最新告警时间、重复次数。

7.3 技术服务要求

7.3.1 集成实施要求

7.3.1.1 总体要求

中标方负责本项目软硬件总集成服务工作，含与主站系统、现有系统、机房布线、通信通道等工作。根据初步设计方案，提供平台软件和硬件总集成部署方案。

中标方配合贵州电网公司开展验证测试、联调测试、第三方测试/测评等，以及与主站系统建设项目的联调测试，协助业主督促主站应用功能建设软件开发商、平台商按集成方案实施，确保满足初步设计要求和系统建设要求。

本项目系统集成与实施，包含安装材料购置，自动化机房内相关布线、设备上电、跳接、安装、配置、联调等工作，与主站系统的联调和运行优化，实现计量自动化系统主站正常稳定地运行。中标方在每一项工作前分析需求，确定方案和实施步骤，实施过程记录，实施后进行优化配置并备份。中标方负责根据自身的产品特性提供准确的现场拓扑结构和切实可行的深化图纸。

在“贵州电网公司计量自动化系统3.0建设”项目验收的各个环节（如到货验收、现场验收及竣工验收）根据相关技术规范进行。本项目建设与主站应用功能建设、机房配套建设、通信配套建设紧密相关，各建设部分的竣工验收需同步进行。

7.3.1.2 集成实施主要要求

本项目软硬件设备到货后，中标方根据集成方案完成软硬件集成工作，实现主站系统软件所需平台环境的配置和集成联调，满足主站系统稳定正常运行和业务应用需求的环境。中标方应在每一项工作前分析需求，确定方案和实施步骤，实施过程记录，实施后进行优化配置并备份。工作涵盖边缘集群中的安全接入区、安全Ⅰ区、安全Ⅱ区、安全Ⅲ区含边界的设备配置和联调，具体工作包括但不限于如下内容：

(1) 中标方负责生产环境、开发测试环境等相关环境部署，通过租户+资源隔离的形式实现生产环境外的环境搭建；

(2) 中标方负责完成本项目所有软硬件资源的软硬件安装、配置、调试等工作，配合第三方测试、等保测评及安全防护评估、商用密码应用安全性评估（含商用密码方案评审）、安全检测（含入网安全评测、源代码审计）、渗透测试、电力监控系统安全风险评估等安全测评需要，并负责相关安全问题的整改，负责平台部分通过相关安全测评，并配合主站系统整体通过相关评测；

(3) 购置软硬件资源安装配置、联调等所需的，机房工程标包所提供的超六类网线和万兆光纤之外的线材、光模块等其他辅助材料；

(4) 设备搬运、清洁、上架、安装、加电、标签标识等工作；

(5) 实施机房内设备相关的网线或光纤的布线及标签标识等，配套机房工程的综合布线不满足平台部署要求的，需中标方按照配套机房工程的建设要求，进行综合布线；

(6) 中标方涉及的采购范围内交换机、服务器、堡垒机、数据库审计、卫星时钟等所有设备的策略配置、参数配置以及测试和优化工作；

(7) 中标方负责完成平台设备与其他设备之间的集成联调，包括不在本标的采购范围的设备，例如：态势感知系统采集装置等装置的集成联调，保障主站系统正常运行；

(8) 中标方负责完成与现有系统、数据分析域的设备连线、配置和联调，若现有系统、数据分析域设备缺少通信的模块等辅助材料，也含在中标方的供货范围之内，中标方负责与现有系统、数据分析域的通信通道联调并保障系统的正常运行；

(9) 中标方负责协助机房工程实施人员完成与通信设备的连线，配合进行配置和联调，以及提供该项工作相关的线材、光模块等辅助材料，并配合配套通信工程的实施，负责主站系统的各类网络通道联通联调，保障主站系统的各类网络通道的正常运行；

(10) 中标方负责平台操作系统安装、配置以及优化；

(11) 中标方负责完成虚拟机、容器、网络环境等相关组件、能力的建设，并配合主站应用功能建设厂家完成主站应用程序的部署；

(12) 中标方负责完成微服务的框架搭建，并配合主站应用功能建设厂家完成微服务的部署；

(13) 中标方负责各类数据库及数据库集群的搭建、测试和优化配置，同时负责数据库之间的数据同步和数据一致性校验，协助主站应用功能建设厂家完成数据库的数据库规划和数据模型建设；

(14) 中标方负责数据计算组件的数据存储规划和集群搭建，并对大数据集群运行进行调优；

(15) 中标方按照云边协同的规范要求，与调度云节点（数据分析域）建设厂家协同，实现调度云节点（数据分析域）和边缘集群（采集监控域）之间的集成联调；

(16) 中标方负责实现本项目所有资源监测信息的传输和联调等；

(17) 中标方完成与本项目采购的软硬件及相关的利旧软硬件（含本项目框采设备）等设备接入到调度态势感知采集装置，并确保将态势感知数据上送至态势感知主站；

(18) 中标方配合主站集群的搭建，含负载均衡器配置、测试和优化配置；

(19) 平台上线、割接、实施、调试、试运行、验收等整个环节均需中标方指派专人配合。

7.3.1.3 软硬件设备实施步骤要求

7.3.1.3.1 设备到货验收

在工程正式开始施工之前，根据合同清单，首先对所到贵州电网公司现场的设备进行设备到货验收工作，该验收工作由双方、监理方共同进行开箱检验，主要检查内容包括设备的外包装、设备外观、数量、型号、设备状况等，经贵州电网公司核对审核无误后，双方签署“设备到货验收单”即“设备收货单”，然后施工人员开始进入设备的安装调试阶段。

7.3.1.3.2 设备上架和安装

根据机柜布局设计对设备进行上架安装工作，在施工过程中要求做到以下规范。

设备安装施工人员必须遵循的人身安全规范和设备操作安全规范，避免在操作设备时，造成人身伤害或设备损坏。

(1) 警告和安全标识

维护设备时，需要遵循警告和安全标识提示的注意事项，避免造成人身伤害或设备损坏。

(2) 静电防护

在进行设备的安装、维护等操作时，需要遵循防止静电的安全注意事项，避免造成人身伤害或设备损坏。

(3) 安全使用激光

在进行设备的安装、维护等操作时，需要遵循使用激光的安全注意事项，避免造成人身伤害或设备损坏。

(4) 安全使用光纤

安全正确地使用光纤，确保设备正常运行，避免造成人身伤害或设备损坏。

(5) 短路防护

在进行设备的安装、维护等操作时，操作工具的使用和放置应遵守工具操作规范，避免操作工具等金属物体造成设备短路。

(6) 安全带电操作

在进行设备的安装、维护等操作时，需要遵循安全带电注意事项，避免造成人身伤害或设备损坏。

7.3.1.3.3 硬件设备集成及测试

硬件设备集成及测试的具体安装实施过程以集成实施方案和最终的交付文档为准。

7.3.1.3.4 网络互联

网络互联涉及设备与交换机互联，交换机与交换机互联等，此处只针对需求提出建议，实际设备互联实施应包括设备具体的配置要求，且与相关厂家工程师沟通后的实施方案为准。

(1) 设备与交换机互联要求业务网络双冗余交换线路接入，提高接入可靠性；

(2) 相同安全区域和相同工作类型的设备分别上架安装在临近的机柜；

(3) 交换机之间互联链路以 2 条及以上的端口进行端口聚合，配置为 Trunk。

7.3.1.3.5 服务器安装和测试

服务器安装和测试具体安装实施和测试过程以集成实施方案和最终的交付文档为准。

7.3.1.3.6 项目验收

本项目与主站应用功能建设、机房配套建设、通信配套建设紧密相关，各建设部分的竣工验收需同步进行。

7.3.1.4 网络安全实施要求

本项目需要满足国家和南方电网公司的网络安全管理要求，包含但不限于以下要求。

7.3.1.4.1 密码安全要求

本项目所有账号的密码设置必须遵循以下策略：

(1) 密码必须满足复杂性要求，包含大小字母、数字和特殊字符；

(2) 密码长度必须大于 12 及以上；

(3) 设置账号口令生存周期是 90 天；

(4) 设定密码历史，不能重复使用最近 5 次内已使用的口令；

(5) 不得有空密码账号存在。

7.3.1.4.2 账号安全要求

系统上线后实施以下策略：

(1) 各个系统需要评估和锁定可能无用账户；

(2) 删除可能无用的用户组；

(3) 设定账号锁定策略：认证失败锁定账户时间为 10 分钟，认证失败锁定账户的最大次数为 6 次；

(4) root 用户不得远程 SSH 登录；

(5) 字符交互界面账户超时 10 分钟自动退出；

(6) 图形界面设置默认自动锁屏时间为 10 分钟。

7.3.1.4.3 操作系统安全要求

用漏洞扫描工具扫描操作系统漏洞，关闭无用端口，关闭影响信息安全的策略。

7.3.1.4.4 日志配置要求

(1) 数据库应配置日志功能，对用户登录进行记录，记录内容包括用户登录使用的账号、登录是否成功、登录时间以及远程登录时用户使用的 IP 地址。

(2) 数据库应配置日志功能，记录用户对数据库的操作；

(3) 通过设置让系统记录安全事件，方便管理员分析。

7.3.1.4.5 通信和其他安全设置

(1) 设置只有信任的 IP 地址才能通过监听器访问数据库；

(2) 使用提供的高级安全选件来加密客户端与数据库之间或中间件与数据库之间的网络传输数据；

(3) 为数据库监听器的关闭和启动设置密码；

(4) 数据库将自动断开超过 10 分钟的空闲远程连接。

7.3.1.4.6 数据库逻辑误操作防范要求

(1) 严格设置生产系统和测试系统，保持两套系统数据库版本的一致性；

(2) 禁止直接在生产系统上以超级管理员或 DBA 等高级权限身份通过手工输入脚本的方式来执行数据库的运维工作；在生产系统上运行的脚本，必须先在测试系统上验证完成后方可在生产系统上执行；

(3) 实施和正式运行阶段，需要定期做好数据的备份，特别是核心数据（如用户档案、月冻结数据等）需要做好定期全量备份，并保持多份数据全备份存储，以便在发生逻辑误操作时（如全库删除）能够最大限度地恢复数据，降低数据丢失的损失。

7.3.1.4.7 其他安全要求

(1) 禁用不必要的系统服务，如 NIS/NIS+、打印服务、sendmail 等；

(2) 禁止 SNMP 弱口令。

7.3.1.5 与主站系统的集成要求

中标方要求按项目设计方案进行平台开发、部署和建设，中标方除负责本项目的开发实施、平台部署、测试、试运行等工作外，还需要配合主站应用功能建设厂商进行相关的系统优化，确保程序开发部署及总体联调均符合设计方案的各项要求，包括系统架构、组件使用要求、程序开发要求、数据存储要求、计算架构要求、数据流控制流要求等相关实施要求，满足海量数据存储及计算要求。

中标方应在贵州安全III区提供贵州各安全分区的“云计算平台资源监测信息及配置信息、虚拟机资源监测信息、微服务监测信息、容器资源监控信息、安全管理中心监测信息”等，并提供接口实现与主站应用功能建设厂家进行内部数据交互。云计算平台厂家应配合主站应用功能建设厂家完成接口联调工作。

7.3.1.6 实施技术服务要求

7.3.1.6.1 现场技术支持服务

驻场服务要求（含日常巡检的）包括缺陷更正，主站应用开发的技术支持，测试、检查、问题变更等支撑，提供变更报告、版本升级报告、巡检报告。服务范围包括本次采购的所有软硬件资源。

本项目软硬件安装开始到“贵州电网公司计量自动化系统 3.0 建设”项目整体竣工验收完成，需提供至少 6 人每周 5x8 小时的计量自动化系统分布式平台、虚拟化技术平台、智能应用软件、应用性能管理软件原厂（提供社保证明）现场技术支持服务。

由贵州电网公司安排适当时间，中标方负责派技术专家到贵州电网公司现场作技术服务。中标方技术服务人员在现场除了应解答和解决由贵州电网公司在合同范围内提出的问题外，还应详细解答图纸、设备性能以及设备运行注意事项。

完成设备上架安装、配置和调试，以及软件功能安装、调试，完成数据整合及必要的图形、模型、数据录入、数据核对等工程量工作，并配合验收。

具体要求如下：

(1) 技术支持的范围涵盖系统中所有由中标方提供的以及用户委托中标方维护的软件。

(2) 若贵州电网公司或用户人员无法解决故障，中标方派维护人员到现场处理。紧急情况下，维护人员要在 4 小时内到达。

(3) 中标方根据解决问题所需的专门技术，派遣专人处理紧急事件。

(4) 提供模块更换服务，更换故障部件。对于发生故障的硬盘，不允许收回故障硬盘，故障硬盘由贵州电网公司自行处理。

(5) 对于紧急递送的请求，用于更换的部件在 24 小时内送达。

(6) 中标方提供的技术维护服务不得免除中标方所负的质量保证责任。

(7) 紧急技术支持可采用远程拨号上网在线诊断的方式。

(8) 中标方推荐适用于系统的测试设备与专用工具，用户方购买后用以维护内部使用的硬件或软件。中标方或其它供货商需提交推荐的测试设备与工具的列表给贵州电网公司，并附目录和采购信息。

7.3.1.6.2 技术支持服务人员要求

技术支持服务人员要求如下：

(1) 投标文件应该包含现场技术支持服务人员的有效证件；

(2) 对本项目采购的各组件资源开通、日常变更、日常问题处理；

(3) 对本项目建设内容进行日常巡检，确保平台稳定运行；

(4) 对本项目建设的各设备、组件的问题进行排查、诊断、定位和修复，和二线工程师对接，直至恢复组件基本功能正常运行；

(5) 对用户如何正常地使用本项目建设的各设备、组件进行指导；

(6) 了解用户需求，对平台进行优化，提升用户体验；

(7) 熟悉计量自动化系统分布式平台、虚拟化技术平台、智能应用组件、应用性能管理组件等本项目采购的各软硬件的运维；

(8) 计量自动化系统分布式平台、虚拟化技术平台驻场服务人员同时具备两个条件，1）分布式平台、虚拟化技术平台原厂认证和授权的合作伙伴工程师，通过原厂平台计算专业认证考试，需提供证书电子版；2）驻场服务人员同时具备近四年负责过 2 个同类型分布式平台、虚拟化技术平台运维项目业绩，需提供甲方证明或合同关键页证明（含对应人员名称）；

(9) 智能应用软件、应用性能管理驻场服务人员具备两个条件之一，1）原厂认证和授权的合作伙伴工程师，通过原厂平台计算专业认证考试，需提供证书电子版；2）驻场服务人员同时具备近四年负责过 2 个同类型分布式平台、虚拟化技术平台运维项目业绩，需提供甲方证明或合同关键页证明（含对应人员名称）；

(10) 具有采集系统类分布式平台、虚拟化技术平台运维经验人员优先考虑，需提供证明材料；

(11) 3 年以上相关工作经验。

技术团队实力：计量自动化系统分布式平台软件原厂商人员，按项目人员资质、技术负责人的水平、人员配备情况提供材料：

说明：

（1）人员资质方面：高级人员需具备信息系统项目管理师（高级）或网络规划设计师或系统分析师或系统集成项目管理工程师（中级）或 PMP 或 IPMP 其中至少 1 个证书。中级人员需具备分布式平台软件原厂商资质认证证书。应提供证书复印件并加盖投标人公章（允许使用投标专用章或电子章）或分布式平台软件原厂商公章（不允许投标专用章及电子章）；按符合以上条件的参与本项目高级人员数量优先排序，再按中级人员数量排序。

（2）技术负责人水平方面：需配备 1 名分布式平台软件原厂商架构师作为项目技术负责人，硕士及以上学历，同时兼具有分布式平台软件原厂商的云产品架构师相关认证，应提供证书复印件并加盖分布式平台软件原厂商公章（不允许投标专用章及电子章）；项目负责人在满足以上条件的基础上，提供其负责的云平台实施项目清单，提供相关项目合同首页、个人信息页、盖章签字页等扫描件。

（3）人员配备方面：提供加盖分布式平台原厂公章的参与本项目原厂人员清单（包括以上两项的人员），按照学历或同等职称排序，且所列人员需提供本单位近三个月社保证明。

7.3.2 包装运输

7.3.2.1 总体要求

(1) 中标方负责设备的标志、包装、运输，并严格按 GB/T 3873 规定执行。

(2) 包装和运输均在工厂验收完成后进行。

7.3.2.2 包装

中标方提供的所用合同设备应包装牢固，保证设备免受腐蚀雨淋和振动。包装应能承受大批量搬运、装卸以及长距离空运、陆运运输。保证设备安全抵达贵州电网公司现场而无损坏。设备包装应符合下述条件：

(1) 所有设备包装应便于装卸、转运和现场安装。

(2) 在运输和存储期间，设备的电气绝缘应防止受潮和灰尘进入。

(3) 对于那些受冲击和振动易于损坏的设备，中标方应按要求以适用于运输的方法包装。

7.3.2.3 运输及搬运

(1) 从中标方所在地到贵州电网公司指定目的地的运输由中标方负责。在设备抵达目的地后，中标方组织贵州电网公司参加开箱验收。如果发现任一设备有偏差、损坏、损失、遗漏或数量、质量、技术规范因中标方的责任与合同不符，贵州电网公司有权向中标方提出换货或索赔。

(2) 最终验收完成之后，中标方代表将设备移交贵州电网公司进行贮存。

(3) 设备可能存在分批发货的要求，中标方需无条件按照贵州电网公司的相关要求分批次发货。

(4) 中标方应按照贵州电网公司的要求，将设备搬运到贵州电网公司指定地点，指定地点包括贮存地点、调试地点及设备正式部署地点等。

7.3.2.4 包装运输搬运费用

项目建设过程中涉及的设备的包装、运输、搬运责任，所需的费用（含包装、运输、搬运、保险等）应包含在总报价中。

7.3.3 开发测试工具的条件

为了保证测试的公正性，系统将采用第三方和中标方提供的专业测试软件，对相应的内容进行测试。

中标方提供的测试工具至少包括平台资源测试工具：采用专业的软件或硬件测试工具，对本项目中的各类软件、设备测试在各类测试条件环境下的系统指标。

7.3.4 开发测试环境的搭建

在中标后 30 天内在业主指定机房中完成开发测试环境搭建。中标方负责提供开发测试环境所需的资源，环境应采用风冷的制冷模式，并提供不少于生产环境的 20%的可用资源，包括但不限于服务器、交换机、云平台基础组件、协同开发平台等全套的软硬件环境，软件版本应与生产环境保持一致。中标方应负责提供开发测试环境搭建所需的耗材，并负责实施和配置等工作，均由中标方自行评估并在投标文件明确罗列，开发环境应能保证主站应用功能建设开发厂家在系统上线前的正常开发、测试等工作。并且承诺后续可以免费迁移至计量检定中心机房。

此项工作所需的相关建设和实施内容含在投标报价中。

7.3.5 AI 环境搭建

中标方负责搭建一套可以支撑业务人工智能应用的大模型环境，支持多模态、图像

识别、语音识别、语义识别等，协助贵州电网公司开展大模型的业务应用训练等工作。

此项工作所需的全部软硬件、配件、实施等建设内容应包含在本次投标报价中。

7.3.6 实现系统启停控制

中标方负责本项目的系统启停控制，在机房断电，UPS 即将失效等极端情况下，通过计划性下电关闭各集群和软硬件，时间不可超过 50 分钟，并保证数据不丢失。在系统可以恢复运行后，通过计划性上电开启各集群和软硬件，时间不可超过 40 分钟。

在计划性下电过程中，需提前通知所有用户和服务，进行关键数据的备份，然后按照优先级逐步停止应用程序、正确关闭数据库等，以及按照正确的顺序关停分布式平台和大数据平台的各个节点。最后，在所有软件层面的操作完成后，切断 UPS 电源。

在计划性上电过程中，检查所有硬件是否完好无损，按预定顺序恢复硬件电源，通常先启动网络设备和存储系统，再启动计算节点，并密切监控每台机器的启动过程，记录遇到的问题。随后，在硬件加电之后，验证系统的状态，包括确认所有必要的服务已经启动并运行正常，用户可以登录且虚拟机状态正常，文件读写无障碍，IP 可达；尝试创建新的虚拟机和云硬盘以确保资源创建功能正常；登录大数据管理平台执行简单的作业调度任务，确保其能正常工作，并检查性能监控工具报告的数据是否符合预期。

7.3.7 培训、技术支持及平台技术标准及规范

为保证贵州电网公司快速了解本项目的部署和运维，中标方需要提供相关技术支持及定制化开发服务，直到系统正式上线，业务应用正常使用。中标方需要提供平台的开发、使用技术规范，指导业主建立未来深入业务开发的技术标准和规范。

针对计量自动化系统分布式平台技术，中标方需面向最终用户提供培训，包括但不限于数据分析、云平台运维管理、功能应用自定义开发（低代码）等等，并协助贵州电网公司完成行业认可的培训成果交付，如主流分布式平台厂家官方认可的行业证书、授权证书，相关培训成本由中标方承担。

7.3.7.1 培训要求

为了确保贵州电网公司更好的履行相关职责，中标方需为贵州电网公司提供设备和系统维护的工具与培训。

(1) 培训班的教员具备：① 教学经验；② 教学课程的专长；③ 熟悉本次招标的系统。

(1) 有关数据库、画面显示、报表生成的用户培训必须使用中文在贵州电网公司授课。

(2) 中标方提供所有培训资料。

(3) 培训课件，中标方在培训前，必须从贵州电网公司的角度出发，准备适用于贵州电网公司不同级别培训的课件（课件形式不限于 PPT），在培训开始前的一个月发贵州电网公司审核，贵州电网公司具有选择拷贝电子课件的权利。

(4) 学员人手一份技术手册和相关文件。学员在培训课程开始前一个月收到教学资料。中标方的手册与文档的电子文件同时提供给贵州电网公司。

(5) 课堂资料，包括开课前发放的文档和课堂资料归贵州电网公司所有，贵州电网公司有权拷贝这些资料供内部培训使用。

(6) 培训内容，包括培训中使用的电子文档提交给贵州电网公司供其内部使用。

(7) 培训的课堂讲授与上机实践要适当平衡，确保学员对课程的充分理解消化。

(8) 中标方提供充足的培训设备，避免出现学员共用一套培训设备的情况。

(9) 对于涉及系统所采用的第三方产品或技术的培训，要求由中标方联系原厂商或由其官方正式授权的培训服务机构提供培训，不能仅由代理机构提供相关培训，其它要求同上述第 1 条到第 9 条。

(10) 必须保证培训质量。培训质量由参加培训人员打分评价，如果评价结果为不合格，则培训提供方需重新安排培训教员免费重新培训，直到培训合格为止。

(11) 培训后应开展受主流技术厂家认可的考核或认证，确保参训人员培训成果得到落实。

7.3.7.2 培训内容

中标方应负责对贵州电网公司进行差异化、针对性的培训，培训主要分为五大类培训，系统概述性培训、硬件维护培训、系统管理员级培训、维护工程师培训、操作人员培训。

(1) 系统概述培训

1．系统入门级培训，从宏观方面介绍整个系统的架构设计原理及原因，新建系统与传统系统的区别及优势；

2．对系统各功能模块做概要性的介绍；

3．通过系统概述性的培训对系统各功能模块的实现机理有初步认识。

(2) 系统管理员培训：

1．平台接口及通讯方法；

2．平台系统的安装、使用、维护等；

3．云服务软件的安装、使用、维护等；

4．网络通信管理及维护；

5．系统支撑软件及应用软件的安装、使用、维护，包括系统的生成、配置、调整和诊断等；

6．演示构建完整系统软件和局部系统的创建方法，包括系统的生成、配置、调整和诊断等；

7．介绍源程序到应用程序的生成、性能设置以及应用函数的参数设置等；

(3) 维护工程师培训：

1．各功能模块介绍；

2．系统平台的一般使用方式；

3．系统安装、生成、维护；

4．图形、报表、安全系统等工具的使用方法；

5．应用软件培训，应用软件与数据流的结构，设计标准和程序节点规范，函数的功能、设计与主要算法，日常维护方法；

(4) 操作人员培训

该课程适合与没有编程经验的学员，主要进行系统数据库、人机界面、报表以及各项功能的使用，使学员熟练掌握各类操作工具并能熟练使用各项功能。

7.3.7.3 培训安排

中标方向贵州电网公司提供的技术培训地点为中标方所在地、贵州电网公司所在地及贵州电网公司指定地点，培训包括原厂培训、现场培训等。相关费用应包含在总报价中。

中标方应根据贵州电网公司的要求及工程进度制定详细的培训方案（包括时间、地点、培训内容、授课人员、建议参加人员等），并在合同谈判上提出培训实施计划并与贵州电网公司磋商。

7.3.7.4 培训计划

(1) 培训计划与进度表要求针对贵州电网公司的需要专门制定。要确保和项目进度表相一致，以保证贵州电网公司人员及时履行职责。

(2) 培训计划需明确区别标准课程（可定期培训）与专为用户准备的课程。

7.3.8 资料提交要求

中标方资料的提交应及时充分，满足工程进度要求。在合同谈判日或收到中标通知书后（以先到为准）根据约定时间给出全部最终技术资料，经业主确认后不能更改。

中标方应在技术协议签订后的约定时间向业主提供正式版的用于设计、设备监造和检验、现场安装和调试以及运行维护方面的图纸、说明书和有关技术资料，同时向贵州电网公司设计代表提供拷贝磁盘 2 份（图纸为 AutoCAD、VISIO 版、文字资料为 WPS、Word 版）。

中标方应提供项目完整的文档资料。文档应包含设计、运行、维护和测试、培训资料以及本规范书中要求的所有文档资料。

中标方应对其所提供的全部文档的准确性和完整性负责。所有由中标方采购供货的第三方设备的技术手册的准确性由中标方负责。

系统提供的所有文档必须与实际系统相一致。文档内容的任何不一致均将被视为不符合技术规范要求。

7.3.8.1 文档范围

中标方应按照南方电网有限责任公司要求，提交覆盖各采购模块的详细“一书三册”（功能说明书、检验手册、安装手册、运维手册）。中标方提供的相关文档内容应涵盖且不限于如下要求：

(1) 系统管理员手册。

(2) 用户手册。

(3) 程序员手册以及二次开发支持文件，包括用于进一步开发或扩展的 API 接口，公用程序和函数的调用方法，数据字典等。

(4) 本项目实施技术资料

1．工程实施工作方案；

2．工程施工图（草图）；

3．工程安装配置手册（含系统部署方案及参数配置说明）；

4．故障处理手册；

5．工程管理员手册；

6．工程启停作业指导书；

(5) 工程竣工图（草图）；

(6) 系统结构和配置说明；

(7) 系统功能和系统性能说明；

(8) 网络通信功能及性能参数；

(9) 系统总装说明（设备安装和布置），环境要求、接地要求、安装要求等；

(10) 系统使用操作说明书及手册；

(11) 维护和检修手册、维护和检修指南，包括故障诊断指南；

(12) 测试和调试说明书（包括方法、数量、调试操作步骤等），验收测试细则和验收测试报告等；

(13) 历次联络会、工程实施方案讨论会会议纪要；

(14) 每次系统或功能维护（包括硬件及软件）的维护报告及技术文档；

(15) 中标方采购供货的第三方设备的软件的技术手册及相关资料；

(16) 提供系统配置图，系统数据接收处理的结构图，服务器、网络交换机、安防设备等所有组屏设备的布局图、端子图，系统连接的各种电缆清册，屏柜安装图、接线原理图、端子排图；

(17) 项目工作报告

1．项目阶段性工作报告

2．项目工作总结报告

(18) 各类测试报告

1．出厂功能、性能、安全测试报告；

2．试运行报告

3．第三方源代码检测报告；

(19) 知识产权成果

本项目产生的所有知识产权成果归贵州电网公司所有；

中标方配合招标方协助编写并受理发明专利不少于 20 项、发表或录用核心、EI 或 SCI 论文不少于 12 篇，软件著作权不少于 2 项；

(20) 安全管理制度文件

根据《GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求》)第 3 级安全要求的安全通用要求和云计算安全扩展要求提供安全管理制度初稿；

根据《GB/T 39786-2021 信息安全技术信息系统密码应用基本要求》第 3 级安全要求提供密码安全管理制度初稿；

协助完成以上管理制度的修订等工作；

(21) 其他

中标方所提供的技术文件，其内容必须和所提供的设备一致，当系统改变或更新升级时，中标方应向贵州电网公司及时提供改变、更新升级后的相关文档，应包括修改的内容，修改理由和对系统可能带来的影响等。

贵州电网公司有权复制中标方提供的技术文件，作为系统的维护管理使用。

7.3.8.2 文档提交要求

中标方应提供系统完整的文档资料。文档应包含设计、运行、维护和测试、培训资料以及本规范书中要求的所有文档资料。

中标方应对其所提供的全部文档的准确性和完整性负责。所有由中标方采购供货的第三方设备的技术手册的准确性由中标方负责。

系统提供的所有文档必须与实际系统相一致。文档内容的任何不一致均将被视为不符合技术规范要求。

7.3.8.3 文档编制要求

7.3.8.3.1 语言

(1) 除贵州电网公司同意外，中标方提交的所有文档应用简体中文编制。

(2) 不允许用中文或英文以外的语言提交文档。翻译英文或其它语言的文件必须同时提交中文和原文版本，以供用户审阅，并作最终建造文档的一部分。

(3) 贵州电网公司有权要求中标方将临时文件和（或）其它没有提交英文版本的文件翻译为中文供内部人员使用。

(4) 本节所有要求同样适用于中标方和第三方的文档编制。

7.3.8.3.2 纸质文本和电子文本

所有中标方文档，包括提交的中文版本，必须采用 WPS2019 版本的文本（或表格，视贵州电网公司需求而定）格式提供。提交给贵州电网公司（及其咨询顾问，若有）的

文档审阅版和最终版本必须以纸质和电子两种文本提交。电子格式包括图片、数学公式、备注和修订，不接受手写文本。所有文档按 A4 格式编制和打印，除非有充分的理由，不得包含过大的文件或折叠插页。

图纸如施工图草图、竣工图草图、接线图等必须采用 AutoCAD 或 VISIO 编制。

7.3.8.3.3 文档交付

除贵州电网公司另有规定外，中标方必须向贵州电网公司电邮电子文本，并提供每份文件或图纸一式三份的初稿、修改稿和最终稿的纸质文本。电子文本必须电邮给贵州电网公司指定的人员的邮箱中。中标方必须同时电邮电子文本和一式一份纸质文本给设计方。

提交给贵州电网公司和设计方的文件交付服务必须是相同等级（航空邮件、快递服务、电邮等）。在系统竣工后提交的文本，也必须同时提交给贵州电网公司及设计方。

贵州电网公司和设计方有权编辑和打印项目所有文本供内部使用。

中标方提交给贵州电网公司的所有文档必须附有一封转送函。每份文件上必须注明订单编号、文档编号、图纸编号、修改或发送编号、发布或修改日期等。

7.3.8.3.4 图纸

贵州电网公司不接受“典型”、“标准”或“自定义”图纸，除非其完全适用于本系统。如果中标方采用上述类型的图纸，不适用部分予以删除或在图纸上清楚地注明。如果图纸内含有可选项，清晰地标明适用本系统的选项，不适用选项清晰注明。

7.3.8.3.5 文档装订

中标方提供的手册和其它书面文档必须用活页装订，在活页的书脊上标明卷数和卷名。

每份文件有完整的目录表，该目录包括章节编号、对应章节的起始页码。产品清单列在目录表后面。内容相关的多册文件在每一卷前提供完整的目录。每套文件都提供一个缩写字母。

7.3.8.4 文档审阅和批准

中标方必须将所有移交文档，包括前面明确列出的文档提交贵州电网公司审阅和批准。文档必须按照批准后的文档计划修订稿中的日程表提交。

7.3.8.4.1 审批要求

以下定义两种供审阅和批准的文件：

(1) 标准文件：第三方供货商文件，中标方于中标前编制和使用的无需修改即能适用于本项目的文件。所有中标方制作的标准文件必须完全适用于本项目。如果先前制作的文档不完全适用，或不准确、不完善、或需要修改部分内容等，中标方应按照要求进行相应的完善和修订，该文档将被视为自定义文件。

(2) 自定义文件：所有其它文件，特别是专为贵州电网公司准备、定制或修改的软硬件功能文件和施工方面的文件。

贵州电网公司享有审阅和批准所有标准文件的权力，中标方应对提交文件的完整性、准确性、清晰性和适用性负全责。

自定义文件，包括专为本项目修改的标准文件，贵州电网公司享有完全的审批权，包括审阅和批准文件内容的权利。

贵州电网公司保留驳回任何不完整、不准确、不清晰、与主题不相关、不符合标准的文件（标准文件或自定义文件）的权力。对于任何因为以上理由被驳回的文件，中标方应进行修订并在贵州电网公司要求的时间内重新提交贵州电网公司审阅和批准。

7.3.8.4.2 中标方责任

中标方提交的文档或图纸在经贵州电网公司批准后仍不得免除中标方保证文档正确性以及遵守合同各项规定的责任。中标方不得以任何理由收取额外费用和要求延期提交文档。如果中标方被告知文件中存在错误、遗漏或前后不一致，无论在批准前或批准后，中标方都必须立即修订该不足。

7.3.8.5 文档内容

各种文档的内容简要说明如下：

7.3.8.5.1 软件功能说明文件

(1) 一般要求

软件功能说明文件针对本项目云平台和应用软件，按照子系统和应用程序的类别分别加以详细说明，对于每个子系统，包括：

1．子系统简介及其应用和功能。

2．从贵州电网公司的角度介绍子系统的所有功能，并包括相关的显示，对话菜单和报表格式。

3．主要算法；

4．子系统用户界面的详细说明书，标出相关显示格式，并解释用户操作程序。

5．功能设计文件在合适的地方引用用户手册的相关摘要内容。

(2) 应用程序的功能文件

本项目云平台及相关系统/应用程序的功能及用户界面对于贵州电网公司非常重要。中标方应提供详细的功能设计文件。功能设计文件从贵州电网公司的角度介绍功能，并解释每项功能的用途和操作方法，并提供相关显示的详细布局图，每个区域及其有效值区间的解释说明。采用画面截取方式来说明其操作方法，并解释相应对话框菜单和按钮的用途。为辅助说明，功能设计文件可引用用户手册的相关内容。

7.3.8.5.2 软件设计详细文档

(1) 云平台服务程序及应用程序

软件设计详细文件按子系统对软件功能文档中所给出的功能和应用进行详细说明。每个子系统包括：

1．子系统用途和操作简介；

2．子系统整体结构图，标明其模块、程序和数据流向；

3．子系统每个程序或模块的用途和功能的说明；

4．算法详细说明和解释；

5．数据结构说明

6．软件参数的意义、可选项或可选择值表；

7．程序或功能升级和扩展方法；

8．访问规则以及使用说明。

(2) 网络通信

1．局域网（LAN）使用的协议和系统网络的详细说明，以便贵州电网公司在系统上增加新的节点；

2．系统局域网和网络上的内部数据流；

3．系统和其他外部相关业务系统的通信接口、协议和数据交换。

(3) 系统软件

1．向贵州电网公司提供包含云平台服务、应用程序、诊断程序和其它该系统相关的软件的全部详细文件。

2．所有应用程序接口（API）的详细文件和手册。

(4) 技术架构设计说明书

1．向贵州电网公司提供针对本项目的云平台产品技术架构设计说明书，业务应用供应商将配合提供相应业务架构设计和功能架构设计说明书。

7.3.8.5.3 软件维护手册

中标方向贵州电网公司移交供货范围内设备的软件维护和开发手册，至少包括：

(1) 系统操作手册；

(2) 编程手册；

(3) 软件应用手册；

(4) 诊断软件手册；

(5) 数据库生成和修改手册；

(6) 数据库访问手册（实时、历史和应用数据库）；

(7) 显示生成和修改手册，包括从 VISIO、AutoCAD 系统的图纸输入及其显示整合；

(8) 报表生成手册；

(9) 系统应用程序维护手册；

(10) 系统应用程序开发手册；

(11) 系统包含的商业应用用户手册，如文字处理器，电子表格，浏览器等。

7.3.8.5.4 系统管理员手册

系统管理员手册包括管理系统的配置、性能、运行以及与外部接口必需的所有信息。其至少包括下列信息和说明：

(1) 生成和配置软件；

(2) 系统性能的监控和调节；

(3) 中标方、设备原厂商以及其它 OEM 供应商提供的系统升级；

(4) 系统安全维护；

(5) 故障诊断的使用以及排错。

系统管理员手册对系统的冗余性以及系统切机方案进行说明和解释，包括备份和切机参数的调整方法，以及当系统增加新设备时扩展切机方案的方法。

7.3.8.5.5 用户手册

用户手册采用通俗的语言编写。该手册是专门针对用户编写的，并涵盖系统的所有功能，包括为用户开发和定制的特殊功能。用户手册根据应用范围和其包含功能进行组

织编排，且提供目录和索引以便快速查找相关操作说明。用户手册，包括打印操作手册，便于操作人员理解，方便其进行在线操作。

用户手册不含系统维护和管理信息。有关维护和管理方面的信息包括在系统管理员手册和维护手册中。

与每个功能相对应的显示画面（包括工具栏、对话菜单）作为用户程序说明的主要手段。说明文字中间视需要配有系统最近更新的显示画面，必要时采用彩色画面。用户说明书首先简要介绍目的和功能。然后说明每个显示数据区的作用、每个按钮的作用、对话菜单选项、可输入值范围、操作方法和顺序、错误信息提示以及程序恢复方法。.

7.3.8.5.6 随机手册

对每一设备都应有完整的、装订好的安装图和说明手册，随设备装箱一起运至现场。

7.3.8.5.7 系统安装和卸载手册

中标方向用户提供相关信息手册，以便用户为安装新系统以及系统过渡做好准备。该文件在项目初期移交，以便用户有足够时间完成相关的准备工作。

手册涵盖所有现场准备、系统安装和卸载工作，包括但不限于以下要求：

(1) 设备准备，包括系统的空间、电源要求等；

(2) 设备安装说明书；

(3) 系统单元与外部系统、通信设备以及网络的电缆接线说明书；

(4) 系统过渡的计划和步骤。

7.3.8.5.8 系统应急预案

中标方应配合贵州电网公司编制系统应急预案，以指导贵州电网公司在系统出现异常状况时采取相应的对策。

对预案编制的要求为：

(1) 操作性，实用性强；

(2) 每种预案至少包括如下内容：预案名称；预案目的；预案启动条件；预案响应级别；组织机构及其首要职责建议；需通知及协调的其他部门；厂家联络方式；备品备件要求；预案执行步骤；预案执行流程图等。

7.3.8.6 文档印刷费用

中标方应根据本文件所列的内容将各种文档资料费作为总报价的一部分，如提供的文档不符合要求，贵州电网公司有权要求中标方重新印刷，费用由中标方承担。

8 安全技术方案要求

本技术规范书中要求的安全及配套设备需求清单为最低安全配置要求，投标方应保证所供设备配置能够满足技术规范书中数量、功能、性能和容量等要求，系统和平台均需要保证满足网络安全等级保护测评及商用密码应用安全性评估要求，并负责解决涉及到的安全问题。

8.1 项目安全建设目标要求

开展计量自动化系统 3.0 建设，把握“云大物移智链”为代表的新技术带来新机遇，满足为用户提供可靠、便捷、高效、智慧的现代供电服务体系建设提出新要求，支撑以新能源为主体的新型电力系统建设催生新业务，全面提高业务支撑能力，满足安全防护技术规范要求，保障极端环境下系统的稳定可靠运行。

安全防护总体目标，依据国家和公司网络安全有关要求，贯彻落实“安全分区、网络专用、横向隔离、纵向认证”十六字方针，结合系统面临的风险分析，从边界、网络、应用、主机、终端、业务、监测和机房物理和环境安全等方面采取网络安全防护措施，构建计量自动化系统 3.0 的网络安全防护能力，防范系统发生网络安全事件，切实保障系统安全稳定运行。安全建设目标符合以下要求：

1、本系统应根据《信息安全技术 网络安全等级保护基本要求》)(GB/T 22239-2019)第 3 级安全要求的安全通用要求和云计算安全扩展要求进行建设。需要保证本项目通过网络安全等级保护测评，并负责解决涉及到的安全问题，保证本项目通过网络安全等级保护测评分值达到 85 分及以上。同时，等级保护测评发现的问题，其整改方式为不能采用临时解决方案，应为正式永久的解决方案。

2、应按照《GB/T 39786-2021 信息安全技术信息系统密码应用基本要求》第 3 级安全要求实现密码应用。涉及密码技术的安全设备或防护措施应达到《GB/T 37092 信息安全技术 密码模块安全要求》2 级及以上安全要求。需要保证本项目满足商用密码应用安全性评估要求，并负责解决涉及到的安全问题，保证本项目商用密码应用安全性评估分值达到合格分及以上且密码应用无高风险。同时，国家商用密码测评发现的问题，其整改方式为不能采用临时解决方案，应为正式永久的解决方案。

3、本系统应遵循国家发改委《电力监控系统安全防护规定》（2014 年第 14 号令）以及国家能源局《电力监控系统安全防护总体方案等安全防护方案和评估规范》（国能安全[2015]36 号）等要求，贯彻落实“安全分区、网络专用、横向隔离、纵向认证”十六

字方针。

4、本系统应满足《中国南方电网电力监控系统网络安全技术规范》《南方电网公司网络安全合规库（2022 年版）》《南方电网公司 IT 主流设备安全基线技术规范》等相关要求。

5、本系统按照“同步规划、同步建设、同步使用”原则加强本系统的网络安全防护，确保不发生重大及以上信息安全事件是本系统建设与运行的网络安全防护底线。

6、本系统开发工作遵循南网相关要求，确保源代码符合安全及规范管控要求；支持安全、可控、可靠软硬件环境访问。

8.2 项目安全建设范围要求

依据国家和公司网络安全有关要求，结合系统面临的风险分析，从边界、网络、应用、主机、安全物理环境等方面采取网络安全防护措施，构建计量自动化系统 3.0 安全防护能力，防范系统发生网络安全事件，切实保障计量自动化系统 3.0 安全稳定运行。

计量自动化系统 3.0 主站的安全物理环境建设，由配套机房工程负责，本项目需配合完成设备上架、接线、上电、基础环境安装等工作。

计量自动化系统 3.0 主站的边界内安全防护建设。

计量自动化系统 3.0 主站的边界外安全防护建设，不在本项目范围内。

计量自动化系统 3.0 主站的第三方测试、等保测评及安全防护评估、商用密码应用安全性评估（含商用密码方案评审）、安全检测（含入网安全评测、源代码审计）、渗透测试、电力监控系统安全风险评估工作，及相关的整改工作。

8.3 项目安全本体要求

依据《GB/T 36572-2018 电力监控系统网络安全防护导则》相关要求，构成系统网络安全防护体系的各个模块应实现自身的安全，依次分为电力监控系统软件的安全、操作系统和基础软件的安全、计算机和网络设备及电力专用监控设备的安全、核心处理器芯片的安全，均应采用安全、可控、可靠的软硬件产品。

8.4 网络安全要求

(1) 安全分区包括安全接入区、Ⅰ区、Ⅱ区以及Ⅲ区。

(2) 对于不同区域之间的安全隔离边界，安全接入区与Ⅰ区、Ⅱ区与Ⅲ区之间分别使用正反向物理隔离装置设立区域隔离边界，而Ⅰ区与Ⅱ区、Ⅲ区与综合数据网之间分别使用边界防火墙设立安全防护边界。

(3) 强化网络边界，生产控制大区纵向互联边界部署纵向加密装置、管理信息大区的纵向互联边界应部署防火墙并严格遵循最小化原则、白名单制。

(4) 计量自动化系统主站通过边界防火墙（IPS、反病毒）、云出口防火墙、网络准入设备、态势感知系统采集装置、蜜罐系统等措施实现安全网络边界防护；贵州计量检定中心机房安全III区通过边界防火墙与棠下机房安全III区进行数据交换。贵州计量检定中心基地安全III区和现有观水路机房计量自动化系统2.0安全III区通过边界防火墙进行数据备份、同步。

(5) 通过服务器版安全操作系统、硬件堡垒机、主机安全系统、漏洞扫描、日志审计等措施实现平台侧安全计算环境防护；

(6) 通过云防火墙、云 Web 应用防火墙、服务器版安全操作系统、云堡垒机、漏洞扫描、日志审计、主机安全系统、数据库审计、数据脱敏等措施实现安全计算环境防护；通过安全中心、日志审计、数据库审计等措施构建安全管理中心。

(7) 根据《南方电网公司计量自动化系统及新型电力负荷管理系统网络安全防护专项提升工作方案》，需建设安全III区缓冲域，最小化部署缓冲域内功能模块。贵州计量自动化系统 3.0 基于安全III区云平台资源划分安全缓冲域 VPC，部署接口服务，同时结合云防火墙和安全组等资源与生产 VPC 实现逻辑隔离。

(8) SSL VPN 相关的产品存在安全漏洞与风险，中标厂家需要使用满足本文要求的安全规范产品替代。

8.5 网络安全等级保护要求

根据《信息安全技术 网络安全等级保护基本要求》)(GB/T 22239-2019)第 3 级安全要求的安全通用要求和云计算安全扩展要求，要求投标方根据下述自检要求进行前期自查，填写通用第三级安全要求自检表、云计算扩展第三级安全要求自检表。

在等级保护测评过程中，中标方为主要负责方，与其他相关方紧密配合，保证本项目的网络安全等级保护测评分值达到 85 分及以上。

8.5.1 通用自检要求

通用第三级安全要求自检表

分类	安全控制点	通用第三级安全要求	技术措施
安	物理位	(1)机房场地应选择在具有防震、防风和防雨等能	满足要求

分类	安全控制点	通用第三级安全要求	技术措施
全物理环境	置选择	力的建筑内；	
		(2)机房场地应避免设在建筑物的顶层或地下室，否则应加强防水和防潮措施。	建设在建筑四层，满足要求
	物理访问控制	(1)机房出入口应配置电子门禁系统，控制、鉴别和记录进入的人员	已通过安防系统建设，满足要求
	防盗窃和防破坏	(1)应将设备或主要部件进行固定，并设置明显的不易除去的标识；	已通过支架固定，7S标识建设
		(2)应将通信线缆铺设在隐蔽安全处；	满足要求
		(3)应设置机房防盗报警系统或设置有专人值守的视频监控系统。	已通过安防系统建设，满足要求
		(4)应将设备或主要部件进行固定，并设置明显的不易除去的标识；	已通过支架固定，7S标识建设
	防雷击	(1)应将各类机柜、设施和设备等通过接地系统安全接地；	已建设机房等电位系统安全接地
		(2)应采取措施防止感应雷，例如设置防雷保安器或过压保护装置等。	已建设三级防雷
	防火	(1)机房应设置火灾自动消防系统，能够自动检测火情、自动报警，并自动灭火；	以建设火灾报警及灭火系统，满足要求
		(2)机房及相关的工作房间和辅助房应采用具有耐火等级的建筑材料；	满足要求，满足要求
		(3)应对机房划分区域进行管理，区域和区域之间设置隔离防火措施。	满足要求，满足要求
	防水和防潮	(1)应采取措施防止雨水通过机房窗户、屋顶和墙壁渗透；	已封堵外窗，满足要求
		(2)应采取措施防止机房内水蒸气结露和地下积水的转移与渗透；	已安装保温棉，满足要求
		(3)应安装对水敏感的检测仪表或元件，对机房进	已建设漏水检测系

分类	安全控制点	通用第三级安全要求	技术措施
		行防水检测和报警	统，满足要求
	防静电	(1)应采用防静电地板或地面并采用必要的接地防静电措施；	地面采用防静电地板，满足要求
		(2)应采取措施防止静电的产生，例如采用静电消除器、佩戴防静电手环等	满足要求
	温湿度控制	(1)应设置温湿度自动调节设施，使机房温湿度的变化在设备运行所允许的范围之内	配置有精密空调，具备温湿度自动调节
	电力供应	(1)应在机房供电线路上配置稳压器和过电压防护设备；	配置有 UPS 电源，浪涌保护器。满足要求
		(2)应提供短期的备用电力供应，至少满足设备在断电情况下的正常运行要求；	配置有 UPS 电源后备电池，满足要求
		(3)应设置冗余或并行的电力电缆线路为计算机系统供电。	设置双路并行的电力电缆线路为计算机系统供电，满足要求
	电磁防护	(1)电源线和通信线缆应隔离铺设，避免互相干扰；	不同桥架安装，满足要求
		(2)应对关键设备实施电磁屏蔽。	配置屏蔽机柜，满足要求
安全通信网络	网络架构	(1)应保证网络设备的业务处理能力满足业务高峰期需要；	资源配置，满足系统整体技术指标要求
		(2)应保证网络各个部分的带宽满足业务高峰期需要；	资源配置，满足系统整体技术指标要求
		(3)应划分不同的网络区域，并按照方便管理和控制的原则为各网络区域分配地址；	项目实施
		(4)应避免将重要网络区域部署在边界处，重要网络区域与其他网络区域之间应采取可靠的技术隔	防火墙、纵向加密认证装置、正反向物理

分类	安全控制点	通用第三级安全要求	技术措施
		离手段；	隔离装置
		(5)应提供通信线路、关键网络设备和关键计算设备的硬件冗余，保证系统的可用性。	通信线路主备、防火墙、交换机、SSL VPN、纵向加密认证装置、堡垒机等设备冗余热备
	通信传输	(1)应采用校验技术或密码技术保证通信过程中数据的完整性；	SSL VPN、纵向加密认证装置
		(2)应采用密码技术保证通信过程中数据的保密性。	SSL VPN、纵向加密认证装置
	可信验证	(1)可基于可信根对通信设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	逐步实现
安全区域边界	边界防护	(1)应保证跨越边界的访问和数据流通过边界设备提供的受控接口进行通信；	边界防火墙
		(2)应能够对非授权设备私自联到内部网络的行为进行检查或限制；	网络准入
		(3)应能够对内部用户非授权联到外部网络的行为进行检查或限制；	防火墙
		(4)应限制无线网络的使用，保证无线网络通过受控的边界设备接入内部网络。	网络准入
	访问控制	(1)应在网络边界或区域之间根据访问控制策略设置访问控制规则，默认情况下除允许通信外受控	防火墙

分类	安全控制点	通用第三级安全要求	技术措施
		接口拒绝所有通信；	
		(2)应删除多余或无效的访问控制规则，优化访问控制列表，并保证访问控制规则数量最小化；	防火墙
		(3)应对源地址、目的地址、源端口、目的端口和协议等进行检查，以允许/拒绝数据包进出；	防火墙
		(4)应能根据会话状态信息为进出数据流提供明确的允许/拒绝访问的能力；	防火墙
		(5)应对进出网络的数据流实现基于应用协议和应用内容的访问控制。	web 应用防火墙
	入侵防范	(1)应在关键网络节点处检测、防止或限制从外部发起的网络攻击行为；	入侵防御系统、APT 系统
		(2)应在关键网络节点处检测、防止或限制从内部发起的网络攻击行为；	入侵防御系统、APT 系统
		(3)应采取技术措施对网络行为进行分析，实现对网络攻击特别是新型网络攻击行为的分析；	入侵防御系统、APT 系统（实现对新型网络攻击行为分析）
		(4)当检测到攻击行为时，记录攻击源 IP、攻击类型、攻击目标、攻击时间，在发生严重入侵事件时应提供报警。	入侵防御系统、APT 系统
	恶意代码和垃圾邮件防范	(1)应在关键网络节点处对恶意代码进行检测和清除，并维护恶意代码防护机制的升级和更新；	防火墙（反病毒模块）
		(2)应在关键网络节点处对垃圾邮件进行检测和防护，并维护垃圾邮件防护机制的升级和更新。	防火墙配置策略关闭 25 端口实现垃圾邮件防护
	安全审计	(1)应在网络边界、重要网络节点进行安全审计，审计覆盖到每个用户，对重要的用户行为和重要	日志审计、数据库审计、堡垒机

分类	安全控制点	通用第三级安全要求	技术措施
		安全事件进行审计；	
		(2)审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	日志审计、数据库审计、堡垒机
		(3)应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等；	日志审计、日志存储服务
		(4)应能对远程访问的用户行为、访问互联网的用户行为等单独进行行为审计和数据分析。	上网行为管理、内网不连接互联网。
	可信验证	可基于可信根对通信设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	逐步实现
安全计算环境	身份鉴别	(1)应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	堡垒机、Ukey、数字证书
		(2)应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	堡垒机、设备设置
		(3)当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听；	SSL VPN
		(4)应采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对用户进行身份鉴别，且其中一种鉴别技术至少应使用密码技术来实现。	堡垒机、Ukey、数字证书
	访问控制	(1)应对登录的用户分配账户和权限；	堡垒机、设备设置
		(2)应重命名或删除默认账户，修改默认账户的默认口令；	堡垒机、设备设置

分类	安全控制点	通用第三级安全要求	技术措施
		(3)应及时删除或停用多余的、过期的账户，避免共享账户的存在；	堡垒机、设备设置
		(4)应授予管理用户所需的最小权限，实现管理用户的权限分离；	堡垒机、设备设置
		(5)应由授权主体配置访问控制策略，访问控制策略规定主体对客体的访问规则；	堡垒机、设备设置
		(6)访问控制的粒度应达到主体为用户级或进程级，客体为文件、数据库表级；	堡垒机、设备设置
		(7)应对重要主体和客体设置安全标记，并控制主体对有安全标记信息资源的访问。	堡垒机、设备设置
	安全审计	(1)应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	日志审计、数据库审计、堡垒机
		(2)审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	日志审计、数据库审计、堡垒机
		(3)应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等；	日志审计、日志存储服务
		(4)应对审计进程进行保护，防止未经授权的中断。	日志审计
	入侵防范	(1)应遵循最小安装的原则，仅安装需要的组件和应用程序；	项目实施
		(2)应关闭不需要的系统服务、默认共享和高危端口；	项目实施
		(3)应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	网络准入
		(4)应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；	通过应用程序校验实现
		(5)应能发现可能存在的已知漏洞，并在经过充分	漏洞扫描

分类	安全控制点	通用第三级安全要求	技术措施
		测试评估后，及时修补漏洞；	
		(6)应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。	主机安全
	恶意代码防范	应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断。	主机安全
	可信验证	可基于可信根对通信设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将 验证结果形成审计记录送至安全管理中心。	逐步实现
	数据完整性	(1)应采用校验技术或密码技术保证重要数据在传输过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等；	服务器密码机、密码服务管理平台
		(2)应采用校验技术或密码技术保证重要数据在存储过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等。	服务器密码机、密码服务管理平台
	数据保密性	(1)应采用密码技术保证重要数据在传输过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等；	服务器密码机、密码服务管理平台
		(2)应采用密码技术保证重要数据在存储过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等。	服务器密码机、密码服务管理平台
	数据备份恢复	(1)应提供重要数据的本地数据备份与恢复功能；	已考虑将 AP 库、关键云服务器备份至

分类	安全控制点	通用第三级安全要求	技术措施
			对象存储
		(2)应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地；	通过云边协同将全量数据备份至数据分析域大数据平台，同时与现有观水路计量 2.0 通过主备同步专线同步数据
		(3)应提供重要数据处理系统的热冗余，保证系统的高可用性。	资源配置，满足系统整体技术指标要求
	剩余信息保护	(1)应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除；	设备设置
		(2)应保证存有敏感数据的存储空间被释放或重新分配前得到完全清除。	设备设置
	个人信息保护	(1)应仅采集和保存业务必需的用户个人信息；	项目实施
		(2)应禁止未授权访问和非法使用用户个人信息。	项目实施
安全管理中心	系统管理	(1)应保证系统管理员通过管理工具或平台进行系统管理操作，并对这些操作进行审计；	堡垒机、系统管理平台
		(2)应通过系统管理员对系统的资源和运行进行配置、控制和管理，包括用户身份、资源配置、加载和启动、运行的异常处理、数据和设备的备份与恢复等。	项目实施
	审计管理	(1)应保证审计管理员通过管理工具或平台进行安全审计操作，并对这些操作进行审计；	堡垒机、系统管理平台
		(2)应通过审计管理员对审计记录进行分析，并根据分析结果进行处理，包括根据安全审计策略对审计记录进行存储、管理和查询等。	日志审计、数据库审计、堡垒机

分类	安全控制点	通用第三级安全要求	技术措施
	安全管理	(1)应对安全管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行安全管理操作，并对这些操作进行审计；	堡垒机、系统管理平台
		(2)应通过安全管理员对系统中的安全策略进行配置，包括安全参数的设置，主体、客体进行统 一安全标记，对主体进行授权，配置可信验证策略等。	项目实施
	集中管控	(1)应划分出特定的管理区域，对分布在网络中的安全设备或安全组件进行管控；	SSL VPN
		(2)应能够建立一条安全的信息传输路径，对网络中的安全设备或安全组件进行管理；	SSL VPN
		(3)应对网络链路、安全设备、网络设备和服务器等的运行状况进行集中监测；	调度态势感知系统采集装置及态势感知系统
		(4)应对分散在各个设备上的审计数据进行收集汇总和集中分析，并保证审计记录的留存时间符合法律法规要求；	日志审计、数据库审计、堡垒机、日志存储服务
		(5)应对安全策略、恶意代码、补丁升级等安全相关事项进行集中管理；	漏洞扫描、主机安全、补丁分发服务
		(6)应能对网络中发生的各类安全事件进行识别、报警和分析。	APT 系统
安全制度	安全策略	(1)应制定网络安全工作的总体方针和安全策略，阐明机构安全工作的总体目标、范围、原则和安全框架等。	安全制度
	管理制度	(1)应对安全管理活动中的各类管理内容建立安全管理制度；	安全制度
	度	(2)应对管理人员或操作人员执行的日常管理操作	安全制度

分类	安全控制点	通用第三级安全要求	技术措施
		建立操作规程；	
		(3)应形成由安全策略、管理制度、操作规程、记录表单等构成的全面的安全管理制度体系。	安全制度
	制定和发布	(1)应指定或授权专门的部门或人员负责安全管理制度的制定；	安全制度
		(2)安全管理制度应通过正式、有效的方式发布，并进行版本控制。	安全制度
	评审和修订	(1)应定期对安全管理制度的合理性和适用性进行论证和审定，对存在不足或需要改进的安全管理制度进行修订。	安全制度
安全运维管理	环境管理	(1)应指定专门的部门或人员负责机房安全，对机房出入进行管理，定期对机房供配电、空调、温湿度控制、消防等设施进行维护管理；	机房管理制度
		(2)应建立机房安全管理制度，对有关物理访问、物品带进出和环境安全等方面的管理作出规定；	机房管理制度
		(3)应不在重要区域接待来访人员，不随意放置含有敏感信息的纸档文件和移动介质等。	机房管理制度
	资产管理	(1)应编制并保存与保护对象相关的资产清单，包括资产责任部门、重要程度和所处位置等内容；	机房管理制度
		(2)应根据资产的重要程度对资产进行标识管理，根据资产的价值选择相应的管理措施；	机房管理制度
		(3)应对信息分类与标识方法作出规定，并对信息的使用、传输和存储等进行规范化管理。	机房管理制度
	介质管理	(1)应将介质存放在安全的环境中，对各类介质进行控制和保护，实行存储环境专人管理，并根据存档介质的目录清单定期盘点；	U 盘使用申请登记，部分符合。如果需要满分需要提供 U 盘加密工具

分类	安全控制点	通用第三级安全要求	技术措施
		(2)应对介质在物理传输过程中的人员选择、打包、交付等情况进行控制，并对介质的归档和查询等进行登记记录。	U盘使用申请登记
	设备维护管理	(1)应对各种设备（包括备份和冗余设备）、线路等指定专门的部门或人员定期进行维护管理；	机房管理制度
		(2)应建立配套设施、软硬件维护方面的管理制度，对其维护进行有效的管理，包括明确维护人员的责任、维修和服务的审批、维修过程的监督控制等；	现场服务报告需要体现
		(3)信息处理设备应经过审批才能带离机房或办公地点，含有存储介质的设备带出工作环境时其中重要数据应加密；	U盘加密工具和U盘解密工具
		(4)含有存储介质的设备在报废或重用前，应进行完全清除或被安全覆盖，保证该设备上的敏感数据和授权软件无法被恢复重用。	机房管理制度
	漏洞和风险管理	(1)应采取必要的措施识别安全漏洞和隐患，对发现的安全漏洞和隐患及时进行修补或评估可能的影响后进行修补；	漏洞扫描
		(2)应定期开展安全测评，形成安全测评报告，采取措施应对发现的安全问题。	系统管理制度
	网络和系统安全管理	(1)应划分不同的管理员角色进行网络和系统的运维管理，明确各个角色的责任和权限；	系统管理制度
		(2)应指定专门的部门或人员进行账户管理，对申请账户、建立账户、删除账户等进行控制；	系统管理制度
		(3)应建立网络和系统安全管理制度，对安全策略、账户管理、配置管理、日志管理、日常操作、升级与打补丁、口令更新周期等方面作出规定；	系统管理制度

分类	安全控制点	通用第三级安全要求	技术措施
		(4)应制定重要设备的配置和操作手册，依据手册对设备进行安全配置和优化配置等；	系统管理制度
		(5)应详细记录运维操作日志，包括日常巡检工作、运行维护记录、参数的设置和修改等内容；	系统管理制度
		(6)应指定专门的部门或人员对日志、监测和报警数据等进行分析、统计，及时发现可疑行为；	系统管理制度
		(7)应严格控制变更性运维，经过审批后才可改变连接、安装系统组件或调整配置参数，操作过程中应保留不可更改的审计日志，操作结束后应同步更新配置信息库；	系统管理制度
		(8)应严格控制运维工具的使用，经过审批后才可接入进行操作，操作过程中应保留不可更改的审计日志，操作结束后应删除工具中的敏感数据；	系统管理制度
		(9)应严格控制远程运维的开通，经过审批后才可开通远程运维接口或通道，操作过程中应保留不可更改的审计日志，操作结束后立即关闭接口或通道；	系统管理制度
		(10)应保证所有与外部的连接均得到授权和批准，应定期检查违反规定无线上网及其他违反网络安全策略的行为。	系统管理制度
	恶意代码防范管理	(1)应提高所有用户的防恶意代码意识，对外来计算机或存储设备接入系统前进行恶意代码检查等；	系统管理制度
		(2)应定期验证防范恶意代码攻击的技术措施的有效性。	巡检记录
	配置管理	(1)应记录和保存基本配置信息，包括网络拓扑结构、各个设备安装的软件组件、软件组件的版本	巡检记录

分类	安全控制点	通用第三级安全要求	技术措施
		和补丁信息、各个设备或软件组件的配置参数等；	
		(2)应将基本配置信息改变纳入变更范畴，实施对配置信息改变的控制，并及时更新基本配置信息库。	台账
	密码管理	(1)应遵循密码相关国家标准和行业标准；	商密应用
		(2)应使用国家密码管理主管部门认证核准的密码技术和产品。	商密应用
	外包运维管理	(1)应确保外包运维服务商的选择符合国家的有关规定；	项目实施
		(2)应与选定的外包运维服务商签订相关的协议，明确约定外包运维的范围、工作内容；	项目实施
		(3)应保证选择的外包运维服务商在技术和管理方面均应具有按照等级保护要求开展安全运维工作的能力，并将能力要求在签订的协议中明确；	项目实施
		(4)应在与外包运维服务商签订的协议中明确所有相关的安全要求，如可能涉及对敏感信息的访问、处理、存储要求，对 IT 基础设施中断服务的应急保障要求等。	项目实施
	变更管理	(1)应明确变更需求，变更前根据变更需求制定变更方案，变更方案经过评审、审批后方可实施；	变更方案
		(2)应建立变更的申报和审批控制程序，依据程序控制所有的变更，记录变更实施过程；	变更流程
		(3)应建立中止变更并从失败变更中恢复的程序，明确过程控制方法和人员职责，必要时对恢复过程进行演练。	变更方案
	备份与恢复管	(1)应识别需要定期备份的重要业务信息、系统数据及软件系统等；	系统管理制度

分类	安全控制点	通用第三级安全要求	技术措施
	理	(2)应规定备份信息的备份方式、备份频度、存储介质、保存期等；	系统管理制度
		(3)应根据数据的重要性和数据对系统运行的影响，制定数据的备份策略和恢复策略、备份程序和恢复程序等。	系统管理制度
	安全事件处置	(1)应及时向安全管理部门报告所发现的安全弱点和可疑事件；	系统管理制度
		(2)应制定安全事件报告和处置管理制度，明确不同安全事件的报告、处置和响应流程，规定安全事件的现场处理、事件报告和后期恢复的管理职责等；	系统管理制度
		(3)应在安全事件报告和响应处理过程中，分析和鉴定事件产生的原因，收集证据，记录处理过程，总结经验教训；	系统管理制度
		(4)对造成系统中断和造成信息泄漏的重大安全事件应采用不同的处理程序和报告程序。	系统管理制度
	应急预案管理	(1)应规定统一的应急预案框架，包括启动预案的条件、应急组织构成、应急资源保障、事后教育和培训等内容；	应急方案
		(2)应制定重要事件的应急预案，包括应急处理流程、系统恢复流程等内容；	应急方案
		(3)应定期对系统相关的人员进行应急预案培训，并进行应急预案的演练；	《应急演练培训签到表》《应急演练签到表》
		(4)应定期对原有的应急预案重新评估，修订完善。	《应急作业指导书》V1.0 和 V2.0

8.5.2 云计算安全扩展自检要求

云计算扩展第三级安全要求自检表

分类	安全控制点	云计算扩展第三级安全要求	标准符合性	技术措施说明
安全物理环境	基础设施位置	应保证云计算基础设施位于中国境内。		
安全通信网络	网络架构	(1)应保证云计算平台不承载高于其安全保护等级的业务应用系统；		
		(2)应实现不同云服务客户虚拟网络之间的隔离；		
		(3)应具有根据云服务客户业务需求提供通信传输、边界防护、入侵防范等安全机制的能力；		
		(4)应具有根据云服务客户业务需求自主设置安全策略的能力，包括定义访问路径、选择安全组件、配置安全策略；		
		(5)应提供开放接口或开放性安全服务，允许云服务客户接入第三方安全产品或在云计算平台选择第三方安全服务。		
安全区域边界	访问控制	(1)应在虚拟化网络边界部署访问控制机制，并设置访问控制规则；		
		(2)应在不同等级的网络区域边界部署访问控制机制，设置访问控制规则。		
	入侵防范	(1)应能检测到云服务客户发起的网络攻击行为，并能记录攻击类型、攻击时间、攻击流量等；		
		(2)应能检测到对虚拟网络节点的网络攻击行为，并能记录攻击类型、攻击时间、攻击流量等；		
		(3)应能检测到虚拟机与宿主机、虚拟机与虚拟机之间的异常流量；		
		(4)应在检测到网络攻击行为、异常流量情况时进行告警。		
	安全审计	(1)应对云服务商和云服务客户在远程管理时执行的特权命令进行审计，至少包括虚拟机删除、虚拟机重启；		
		(2)应保证云服务商对云服务客户系统和数据的操作可被云服务客户审计。		
安全计算环境	身份鉴别	当远程管理云计算平台中设备时，管理终端和云计算平台之间应建立双向身份验证机制。		
	访问控制	(1)应保证当虚拟机迁移时，访问控制策略随其迁移；		
		(2)应允许云服务客户设置不同虚拟机之间的访问控制策略。		
	入侵防范	(1)应能检测虚拟机之间的资源隔离失效，并进行告警；		
		(2)应能检测非授权新建虚拟机或者重新启用虚拟机，并进行告警；		

分类	安全控制点	云计算扩展第三级安全要求	标准符合性	技术措施说明
		(3)应能够检测恶意代码感染及在虚拟机间蔓延的情况，并进行告警。		
	镜像和快照保护	(1)应针对重要业务系统提供加固的操作系统镜像或操作系统安全加固服务；		
		(2)应提供虚拟机镜像、快照完整性校验功能，防止虚拟机镜像被恶意篡改；		
		(3)应采取密码技术或其他技术手段防止虚拟机镜像、快照中可能存在的敏感资源被非法访问。		
	数据完整性和保密性	(1)应确保云服务客户数据、用户个人信息等存储于中国境内，如需出境应遵循国家相关规定；		
		(2)应确保只有在云服务客户授权下，云服务商或第三方才具有云服务客户数据的管理权限；		
		(3)应使用校验码或密码技术确保虚拟机迁移过程中重要数据的完整性，并在检测到完整性受到破坏时采取必要的恢复措施；		
		(4)应支持云服务客户部署密钥管理解决方案，保证云服务客户自行实现数据的加解密过程。		
	数据备份和恢复	(1)云服务客户应在本地保存其业务数据的备份；		
		(2)应提供查询云服务客户数据及备份存储位置的能力；		
		(3)云服务商的云存储服务应保证云服务客户数据存在若干个可用的副本，各副本之间的内容应保持一 致；		
		(4)应为云服务客户将业务系统及数据迁移到其他云计算平台和本地系统提供技术手段，并协助完成迁移过程。		
	剩余信息保护	(1)应保证虚拟机所使用的内存和存储空间回收时得到完全清除；		
		(2)云服务客户删除业务应用数据时，云计算平台应将云存储中所有副本删除。		
安全管理中心	集中管控	(1)应能对物理资源和虚拟资源按照策略做统一管理调度与分配；		
		(2)应保证云计算平台管理流量与云服务客户业务流量分离；		
		(3)应根据云服务商和云服务客户的职责划分，收集各自控制部分的审计数据并实现各自的集中审计；		
		(4)应根据云服务商和云服务客户的职责划分，实现各自控制部分，包括虚拟化网络、虚拟机、虚拟化安全设备等的运行状况的集中监测。		
安全运维	云计算环	(1)云计算平台的运维地点应位于中国境内，境外对境内云计算平台实施运维操作应遵循国家相关规定。		

分类	安全控制点	云计算扩展第三级安全要求	标准符合性	技术措施说明
管理	境管理	(2)应建立数字资产安全管理策略，对数据全生命周期的操作规范、保护措施、管理人员职责等进行规定，包括并不限于数据采集、存储、处理、应用、流动、销毁等过程；		
		(3)应制定并执行数据分类分级保护策略，针对不同类别级别的数据制定不同的安全保护措施；		
		(4)应在数据分类分级的基础上，划分重要数字资产范围，明确重要数据进行自动脱敏或去标识的使用场景和业务处理流程；		
		(5)应定期评审数据的类别和级别，如需要变更数据的类别或级别，应依据变更审批流程执行变更。		

8.6 商密应用要求

8.6.1 项目密码应用需求

依据国家和公司网络安全有关要求，结合系统面临的风险分析，从边界、网络、应用、主机等方面采取网络安全防护措施，构建计量自动化主站系统的网络安全防护能力，防范系统发生网络安全事件，切实保障系统安全稳定运行。

本项目安全防护范围包括安全接入区、安全Ⅰ区、安全Ⅱ区、安全Ⅲ区。应按照《GB/T 39786-2021 信息安全技术信息系统密码应用基本要求》第三级安全要求，从系统的物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全四个层面提出密码应用技术要求，保障信息系统的实体身份真实性、重要数据的机密性和完整性、操作行为的不可否认性；并从信息系统的管理制度、人员管理、建设运行和应急处置四个方面提出密码应用管理要求，为信息系统提供管理方面的密码应用安全保障。涉及密码技术的安全设备或防护措施，均应采用国产商用密码技术，达到《GB/T 37092 信息安全技术 密码模块安全要求》二级及以上安全要求。

8.6.2 项目商密应用安全目标及原则要求

8.6.2.1 安全目标要求

本项目商密应用方案的总体安全目标是依据《GB/T 39786-2021 信息安全技术 信息系统密码应用基本要求》，综合考虑贵州电网有限责任公司计量自动化系统主站的物理和环境、网络和通信、设备和计算、应用和数据、安全管理等层面的密码应用需求，依托商用密码防护技术，对贵州电网有限责任公司计量自动化系统主站进行密码支撑与应

用设计，实现用户终端安全防护、网络接入安全、业务应用安全等方面的密码技术应用。设计合规、正确、有效的系统密码应用方案，最终保障系统在身份识别、安全隔离、信息加密、完整性保护等方面的密码防护，为贵州电网有限责任公司计量自动化系统主站的安全可靠运行提供全面高效的密码支撑，并为通过密码应用安全性评估奠定基础。

8.6.2.2 方案原则要求

计量自动化系统主站密码应用方案应遵循以下原则：

(1) 合规性

国产密码应用须根据《中华人民共和国密码法》《GB/T 39786-2021 信息安全技术 信息系统密码应用基本要求》等相关要求，选择具有国家密码管理局核准的商用密码产品及服务，开展应用系统国产密码应用工作。

(2) 先进性

结合考虑实用和兼顾今后发展的目的，在硬件设备、软件产品等密码产品使用方面，应选择当今市场上主流、领先且稳定的密码产品和技术。

(3) 冗余性

考虑容错能力，关键节点设备和核心设备有适当的冗余，采用灵活的负载均衡机制，避免单点故障导致业务中断，并最大限度减少故障。

(4) 安全性

从网络、系统、应用和管理四个方面综合考虑，采用先进的安全技术，提供完善的安全防护机制，确保数据防篡改、防入侵、司法机关认可法律效力。对于硬件设备，应考虑确保数据不被非法入侵者破坏和盗用，并确保数据的一致性，对欺诈行为应采取多种检查和处理手段。

(5) 总体性

通过从整体层面，从顶层角度，成体系地提供本系统的密码应用方案，并与本系统网络安全保护等级相结合，形成涵盖技术、管理、实施保障的整体方案，为在本系统中落实密码应用相关要求奠定基础。

8.6.3 主要设备和关键数据要求

8.6.3.1 主要密码产品

序号	密码产品名称	涉及的密码算法	主要功能
1	国密服务器密	SM2、SM3、SM4	具有采用国密标准的密码算法芯片，可提供

	码机		数据加解密、完整性校验、密钥生成和管理等能力。支持密码管理服务平台对服务器密码机的独立调用管理。
2	安全门禁系统（在“贵州省级电能检定中心设备及实验室环境项目”中已完成采购）	SM2、SM3、SM4	含密码卡、智能 IC 卡、门禁读卡器，对进入机房人员进行身份鉴别。支持对接视频监控安全管理平台实现商密防护。
3	安全视频监控系统（在“贵州省级电能检定中心设备及实验室环境项目”中已完成采购）	SM2、SM3、SM4	含密码卡，支持音视频信息传输加密和视频文件存储完整性保护。支持对接视频监控安全管理平台实现商密防护。
4	SSL VPN	SM2、SM3、SM4	配合在运维终端（PC）上部署的 VPN 客户端，实现运维终端到服务端之间身份认证、数据传输保护。
5	国密浏览器	SM2、SM3、SM4	部署在用户客户端，实现客户端与服务端之间基于国密算法的网络层身份鉴别、安全通道的建立，实现数据传输机密性和完整性的保护。
6	密码服务管理平台	SM2、SM3、SM4	提供密码服务调度功能，实现密码服务的接入和调度管理；提供密钥管理服务功能，支持密钥全生命周期管理；提供数据加解密、签名验签、身份鉴别等密码服务功能，实现数据的机密性保护、完整性保护等密码安全应用。
7	USB Key	SM2、SM3、SM4	提供签名验签、加密解密、散列等密码运算服务，实现信息的完整性、真实性和不可否认性保护，同时提供一定的存储空间，用于存放数字证书（加密证书、签名证书）。
8	纵向加密认证网关	SM2、SM3、SM4	用于广域网边界防护，为广域网通信提供认证与加密功能，实现数据传输的机密性、完整性保护，具有安全过滤功能。

8.6.3.2 关键数据

序号	关键数据	关键数据描述	安全需求
1	鉴别数据	业务访问用户、应用系统运维用户、基	机密性、完整性

		础环境运维用户的身份鉴别数据（账号、口令）	
2	重要业务数据	应用（费控指令）和云平台的业务数据、虚拟机镜像文件、租户镜像文件、租户快照、配置文件等。	机密性、完整性
3	日志数据	安全设备、网络设备、通用服务器设备、应用系统、云平台等操作日志、运行日志。	完整性
4	访问控制信息	系统访问控制策略、数据库表访问控制信息等。	完整性

8.6.4 商用密码应用方案要求

本密码应用方案应主要包含计算平台密码应用方案(实现物理和环境安全、网络和通信安全、设备和计算安全层面的安全要求)、业务应用的密码应用方案(实现应用和数据安全的安全要求)、密码服务管理平台方案和密钥管理。

其中，计算平台密码应用方案中网络和通信安全、设备和计算安全层面的安全要求以及密码服务管理平台方案，中标方为负责方，中标方应提供满足商用密码应用安全要求的密码产品，并完成产品的实施部署、联调等工作，以满足 GB/T 39786 在网络和通信安全、设备和计算安全层面的安全要求。应提供服务器密码机、密码服务管理平台、数据脱敏、数据水印等等产品的接口给主站应用功能建设开发厂家等第三方调用，配合完成应用和数据安全的密码应用安全建设。同时，涉及到的密钥需满足密钥管理要求，保障系统密码应用的合规性、正确性和有效性。

物理和环境安全、业务应用的密码应用（应用和数据安全）方案主要由机房和通信工程及主站应用功能建设负责，中标方需与其他相关方紧密配合，共同完成系统的密码应用安全建设，满足第三级密码应用基本要求。

第三级密码应用基本要求

分类	第三级密码应用基本要求
物理和环境安全	(1)宜采用密码技术进行物理访问身份鉴别，保证重要区域进入人员身份的真实性；
	(2)宜采用密码技术保证电子门禁系统进出记录数据的存储完整性；
	(3)宜采用密码技术保证视频监控音像记录数据的存储完整性；
	(4)以上如采用密码服务，该密码服务应符合法律法规的相关要求，需依法接受检测认证的，应经商用密码认证机构认证合格；
	(5)以上采用的密码产品，应达到 GB/T37092 二级及以上安全要求。
网络和通信安全	(1)应采用密码技术对通信实体进行身份鉴别，保证通信实体身份的真实性；
	(2)宜采用密码技术保证通信过程中数据的完整性；
	(3)应采用密码技术保证通信过程中重要数据的机密性；
	(4)宜采用密码技术保证网络边界访问控制信息的完整性；

分类	第三级密码应用基本要求
	(5)可采用密码技术对从外部连接到内部网络的设备进行接入认证，确保接入的设备身份真实性；
	(6)以上如采用密码服务，该密码服务应符合法律法规的相关要求，需依法接受检测认证的，应经商用密码认证机构认证合格；
	(7)以上采用的密码产品，应达到 GB/T37092 二级及以上安全要求。
设备和计算安全	(1)应采用密码技术对登录设备的用户进行身份鉴别，保证用户身份的真实性；
	(2)远程管理设备时，应采用密码技术建立安全的信息传输通道；
	(3)宜采用密码技术保证系统资源访问控制信息的完整性；
	(4)宜采用密码技术保证设备中的重要信息资源安全标记的完整性；
	(5)宜采用密码技术保证日志记录的完整性；
	(6)宜采用密码技术对重要可执行程序进行完整性保护，并对其来源进行真实性验证；
	(7)以上如采用密码服务，该密码服务应符合法律法规的相关要求，需依法接受检测认证的，应经商用密码认证机构认证合格；
	(8)以上采用的密码产品，应达到 GB/T37092 二级及以上安全要求。
应用和数据安全	(1)应采用密码技术对登录用户进行身份鉴别，保证应用系统用户身份的真实性；
	(2)宜采用密码技术保证信息系统应用的访问控制信息的完整性；
	(3)宜采用密码技术保证信息系统应用的重要信息资源安全标记的完整性；
	(4)应采用密码技术保证信息系统应用的重要数据在传输过程中的机密性；
	(5)应采用密码技术保证信息系统应用的重要数据在存储过程中的机密性；
	(6)宜采用密码技术保证信息系统应用的重要数据在传输过程中的完整性；
	(7)宜采用密码技术保证信息系统应用的重要数据在存储过程中的完整性；
	(8)在可能涉及法律责任认定的应用中，宜采用密码技术提供数据原发证据和数据接收证据，实现数据原发行为的不可否认性和数据接收行为的不可否认性；
	(9)以上如采用密码服务，该密码服务应符合法律法规的相关要求，需依法接受检测认证的，应经商用密码认证机构认证合格；
	(10)以上采用的密码产品，应达到 GB/T37092 二级及以上安全要求。
建设运行	(1)应依据密码相关标准和密码应用需求，制定密码应用方案；
	(2)应根据密码应用方案，确定系统涉及的密钥种类、体系及其生存周期环节，各环节密钥管理要求参照“密钥生存周期管理”；
	(3)应按照应用方案实施建设；
	(4)投入运行前应进行密码应用安全性评估，评估通过后系统方可正式运行；
	(5)在运行过程中，应严格执行既定的密码应用安全管理制度，应定期开展密码应用安全性评估及攻防对抗演习，并根据评估结果进行整改。
密钥生存周期管理	(1)密钥管理对于保证密钥全生存周期的安全性是至关重要的，可以保证密钥（除公钥外）不被非授权的访问、使用、泄露、修改和替换，可以保公钥不被非授权的修改和替换。信息系统的应用和数据层面的密钥体系由业务系统根据密码应用需求在密码应用方案中明确，并在密码应用实施中落实。密钥管理包括密钥的产生、分发、存储、使用、更新、归档、撤销、备份、恢复和销毁等环节。以下给出各个环节的密钥管理建议供参考。
	(2)密钥产生

分类	第三级密码应用基本要求
	密钥可以以随机产生、协商产生等不同的方式来产生。密钥在符合 GB/T37092 的密码产品中产生是十分必要的，产生的同时可在密码产品中记录密钥关联信息，包括密钥种类，长度、拥有者，使用起始时间、使用终止时间等。
	(3)密钥分发 密钥分发是密钥从一个密码产品传递到另一个密码产品的过程，分发时要注意抗载取、篡改、假冒等攻击，保证密钥的机密性、完整性以及分发者、接收者身份的真实性等。
	(4)密钥存储 密钥不以明文方式存储在密码产品外部是十分必要的，并采取严格的安全防护措施，防止密钥被非授权的访问或篡改。 公钥是例外，可以以明文方式在密码产品外存储，传递和使用，但有必要采取安全防护措施，防止公钥被非授权篡改。
	(5)密钥使用 每个密钥一般只有单一的用途，明确用途并按用途正确使用是十分必要的。密钥使用环节需要注意的安全问题是：使用密钥前获得授权、使用公钥证书前对其进行有效性验证、采用安全措施防止密钥的泄露和替换等。另外，有必要为密钥设定更换周期，并采取有效措施保证密钥更换时的安全性。
	(6)密钥更新 密钥更新发生在密钥超过使用期限，已泄露或存在泄露风险时，根据相应的更新策略进行更新。
	(7)密钥归档 如果信息系统中有密钥归档需求，则根据实际安全需求采取有效的安全措施，保证归档密钥的安全性和正确性。需要注意的是，归档密钥只能用于解密该密钥加密的历史信息或验证该密钥签名的历史信息。如果执行密钥归档，则有必要生成审计信息，包括归档的密钥、归档的时间等。
	(8)密钥撤销 密钥撤销一般针对公钥证书所对应的密钥。当证书到期后，密钥自然撤销；也可以按需进行密钥撤销，撤销后的密钥不再具备使用效力。
	(9)密钥备份 对于需要备份的密钥，采用安全的备份机制对密钥进行备份是必要的，以确保备份密钥的机密性和完整性，这与密钥存储的要求是一致的。密钥备份行为是审计涉及的范围，有必要生成审计信息，包括备份的主体，备份的时间等。
	(10)密钥恢复 可以支持用户密钥恢复和司法密钥恢复。密钥恢复行为是审计涉及的范围，有必要生成审计信息，包括恢复的主体，恢复的时间等。
	(11)密钥销毁 密钥销毁要注意的是销毁过程的不可逆，即无法从销毁结果中恢复原密钥。

8.6.4.1 密码应用总体架构要求

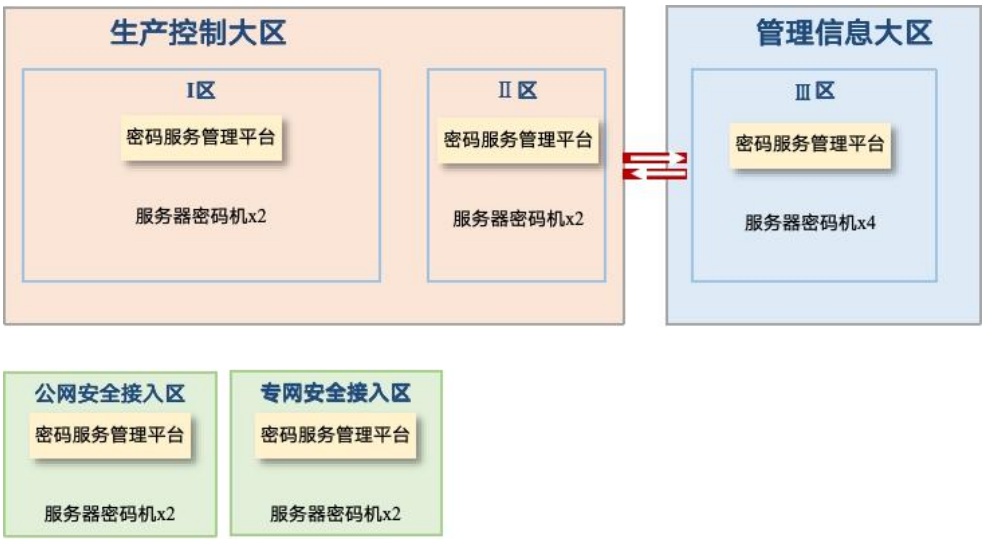

图 8-1 密码应用总体架构示意图

安全接入区、I 区、II 区、III 区的密码服务管理平台分别独立部署和运行；

安全接入区、I 区、II 区、III 区的密码服务管理平台可通过离线方式交换公钥证书，实现跨区的传输加密和认证；

安全接入区、I 区、II 区、III 区的密码服务管理平台对外提供密码功能接口，为业务应用系统、云计算平台实现密码技术的接入。

8.6.4.2 密码应用技术框架要求

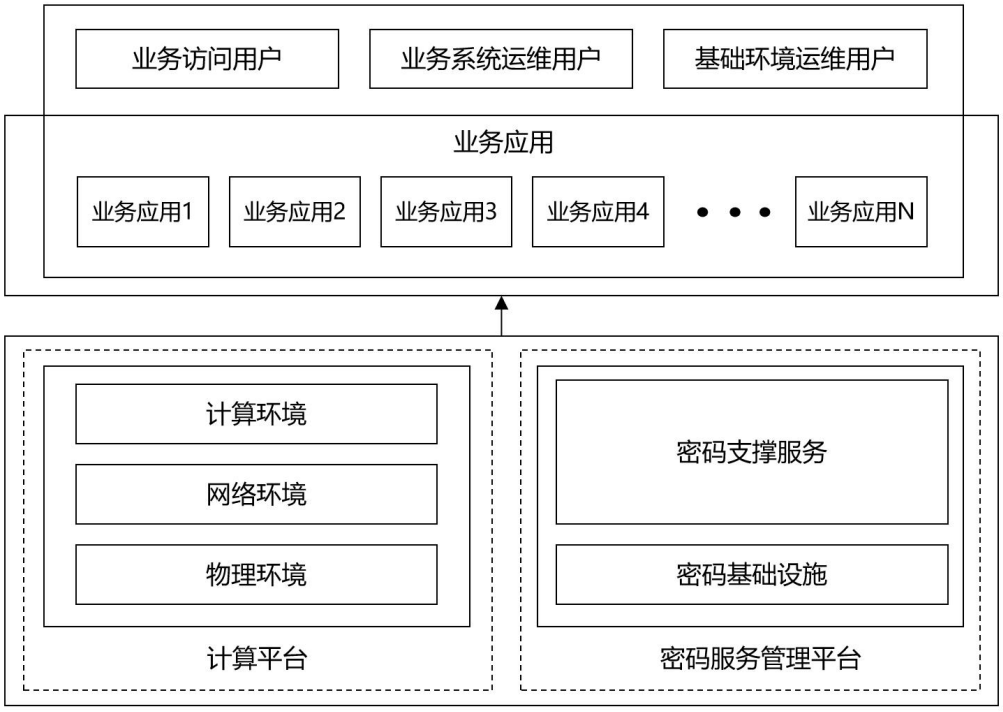

图 8-2 密码应用技术框架图

计量自动化主站系统密码应用技术框架中涉及的计算平台、密码服务管理平台、业务应用和用户如下。

(1) 计算平台

计算平台是承载业务应用的物理环境、网络环境和计算环境。物理环境提供机房、供电、通风、空调、门禁和监控等保障条件；网络环境为业务应用提供数据传输通道和通信设备；计算环境提供承载业务应用运行和数据存储的设备或服务。计算平台使用密码服务管理平台提供的密码功能，为计算平台的运行安全和管理安全提供密码保障。

(2) 密码服务管理平台

密码服务管理平台为计算平台上运行的各类业务应用提供密码支撑服务，该服务以接口的形式提供密码功能，供各业务应用调用，以解决各业务应用的安全问题。密码基础设施为密码应用提供基础支撑。

(3) 业务应用

业务应用是运行在计算平台上，实现业务功能的计算机程序。业务应用的密码应用安全对应 GB/T 39786 中的应用和数据安全。业务应用为解决安全问题需要使用的密码功能，由密码支撑平台提供。计算平台上可运行有多个业务应用，各个业务应用的安全需求各不相同，所以每个业务应用都需要有各自的密码应用设计。

(4) 用户

本系统涉及的用户可分为业务访问用户、业务系统运维用户和基础环境运维用户。业务访问用户是业务应用的使用者；业务系统运维用户是业务应用的所有者和用户的管理者，可管理多个业务应用，各个业务应用可有不同的业务访问用户群；基础环境运维用户是计算平台和密码服务平台的所有者和管理者。

8.6.4.3 计算平台密码应用要求

8.6.4.3.1 物理和环境安全

物理和环境安全保护的对象是业务系统所在机房区域的物理安全，包括进出机房的人员身份真实性、电子门禁系统进出记录数据的存储完整性、视频监控音像记录数据的存储完整性。

8.6.4.3.1.1 身份鉴别

部署符合 GM/T 0036《采用非接触卡的门禁系统密码应用技术指南》要求的机房门禁系统，实现对进出入物理机房人员身份的真实性鉴别。

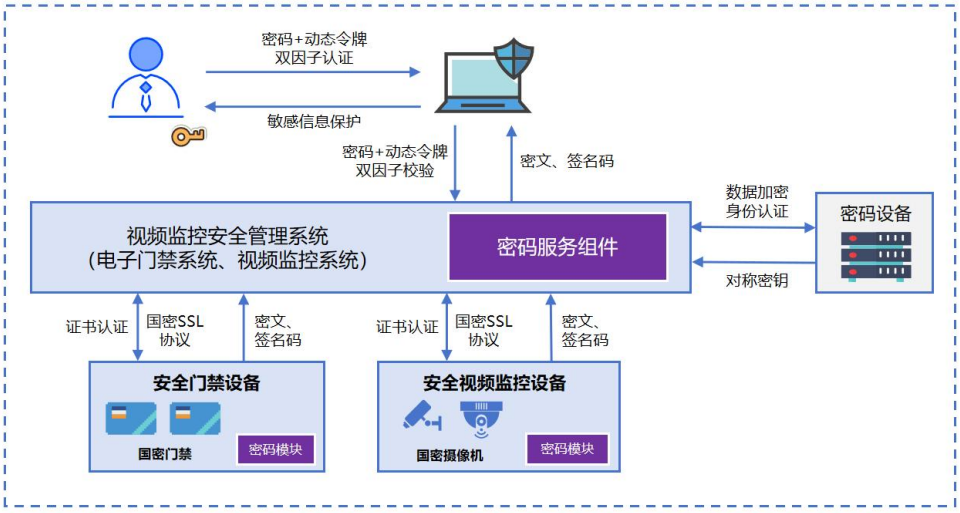

图 8-3 物理和环境安全部署图

8.6.4.3.1.2 电子门禁记录数据和视频监控记录数据存储完整性

电子门禁部署经由国家密码管理部门核准的密码设备，采用基于 SM3 算法的 HMAC 等技术对电子门禁记录、视频监控记录进行完整性保护。

8.6.4.3.2 网络和通信安全

序号	所属安全分区	通道对侧端点	业务需求	对应商用密码应用方案
1	安全接入区	终端	数据采集	采用边界防火墙进行边界防护，采用费控密码机实现身份鉴别，保证通信过程中重要数据的机密性和完整性。
2	安全接入区	计量检定中心机房运维室	实现本计量自动化系统的安全接入区运维	（1）配置国密 USB Key（配套用户数字证书）进行用户身份认证，若设备本身不支持使用配置国密 USB Key 进行用户身份认证的，则通过堡垒机进行运维，禁止直接对设备进行运维操作； （2）使用纵向加密认证网关进行边界防护，采用 SM2/SM3/SM4 算法保证通信过程中重要数据的机密性和完整性。
3	安全接入区	观水路自动化机房安全接入区	通过专线通道实现计量自动化系统 3.0 安全III区和计量自动化系统 2.0 主备采集需求	使用防火墙进行边界防护，通过配置安全策略采用 IPsec 实现隧道加密，保证通信过程中重要数据的机密性和完整性。
4	安全 I 区	计量检定中心机房运维室	实现本计量自动化系统的安全 I 区	（1）配置国密 USB Key（配套用户数字证书）进行用户身份认证，若设备本身不支持使用配置国密 USB Key 进行用户身份认证的，则通过堡垒

序号	所属安全分区	通道对侧端点	业务需求	对应商用密码应用方案
			运维	机进行运维，禁止直接对设备进行运维操作； （2）使用纵向加密认证网关进行边界防护，采用SM2/SM3/SM4 算法保证通信过程中重要数据的机密性和完整性。
5	安全 II 区	调度数据 A 网覆盖的厂站终端	调度数据网 A 网数据采集	使用纵向加密认证网关进行边界防护，配套 USB Key（配置国密证书）实现身份鉴别，采用 SM2/SM3/SM4 算法保证通信过程中重要数据的机密性和完整性。
6		调度数据 B 网覆盖的厂站终端	调度数据网 B 网数据采集	使用纵向加密认证网关进行边界防护，配套 USB Key（配置国密证书）实现身份鉴别，采用 SM2/SM3/SM4 算法保证通信过程中重要数据的机密性和完整性。
7	安全 II 区	计量检定中心机房运维室	实现本计量自动化系统的安全 II 区运维	（1）采用国密 SSL VPN（配置国密数字证书）及配套 VPN 客户端并配置 USB Key（配置用户数字证书），基于数字证书实现客户端和服务端的身份鉴别； （2）终端（PC）上部署 VPN 客户端与国密 SSL VPN 建立基于国密 SSL 协议的安全通信链路。
8	安全 III 区	计量检定中心机房运维室	实现本计量自动化系统的安全III区远程运维	（1）采用国密 SSL VPN（配置国密数字证书）及配套 VPN 客户端并配置 USB Key（配置用户数字证书），基于数字证书实现客户端和服务端的身份鉴别； （2）终端（PC）上部署 VPN 客户端通过专线通道与国密 SSL VPN 建立基于国密 SSL 协议的安全通信链路，使用纵向加密认证网关进行边界防护，采用 SM2/SM3/SM4 算法保证通信过程中重要数据的机密性和完整性。
9	安全 III 区	计量检定中心机房开发室	实现本计量自动化系统的安全III区远程开发测试需求	（1）采用国密 SSL VPN（配置国密数字证书）及配套 VPN 客户端并配置 USB Key（配置用户数字证书），基于数字证书实现客户端和服务端的身份鉴别； （2）终端（PC）上部署 VPN 客户端通过专线通道与国密 SSL VPN 建立基于国密 SSL 协议的安全通信链路，使用纵向加密认证网关进行边界防护，采用 SM2/SM3/SM4 算法保证通信过程中重要数据的机密性和完整性。
10	安全III区	观水路自动化机房	通过专线通道实现计量自动化系统 3.0 安全III区和计量自	使用防火墙进行边界防护，通过配置安全策略采用 IPsec 实现隧道加密，保证通信过程中重要数据的机密性和完整性。

序号	所属安全分区	通道对侧端点	业务需求	对应商用密码应用方案
			动化系统2.0主备采集需求	

8.6.4.3.3 设备和计算安全

8.6.4.3.3.1 本地运维

运维人员通过国密堡垒机，对基础设施、业务系统等进行维护、操作等运维服务。

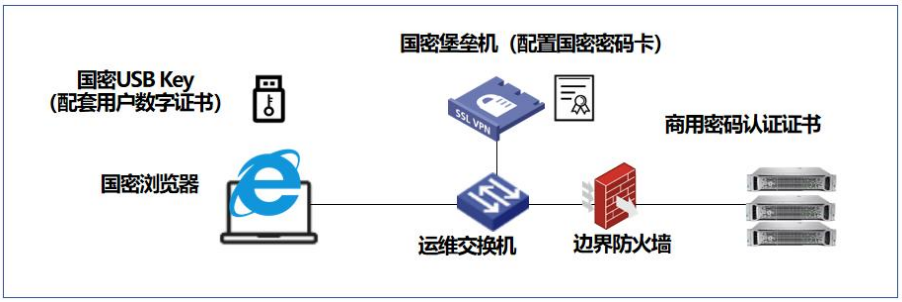

图 8-4 本地运维示意图

8.6.4.3.3.1.1 身份鉴别

针对运维终端（PC），配置国密 USB Key（配套用户数字证书），对登录的用户进行身份鉴别，保证登录用户身份的真实性。

针对国密堡垒机设备（配置国密数字证书），配套 USB Key（配套用户数字证书），基于数字证书实现登录用户身份的身份鉴别。

针对密码类产品（如：服务器密码机、SSL VPN、纵向加密认证网关等），配置国密 USB Key（配套用户数字证书）进行用户身份认证，若设备本身不支持使用配置国密 USB Key 进行用户身份认证的，则通过堡垒机进行运维，禁止直接对设备进行运维操作。

针对通用设备（如：应用服务器、数据库服务器等），则均由堡垒机间接进行运维管理。限制运维人员仅能通过登录堡垒机后才能登录服务器、数据库。

8.6.4.3.3.1.2 资源访问控制信息完整性

针对堡垒机设备，通过配置具有商用密码认证证书的密码卡，实现资源访问控制信息的完整性保护。

针对密码类产品（如：服务器密码机、SSL VPN、纵向加密认证网关、密码服务管理平台等），采用经过商用密码认证机构认证合格的产品，具备相应的安全防护能力，满足相应密码应用需求。

针对通用设备（如：应用服务器、数据库服务器等），逐步实现资源访问控制信息的完整性保护。

8.6.4.3.3.1.3 日志记录完整性

通过日志审计系统对堡垒机、通用设备、密码类产品等日志进行集中采集存储，由业务系统调用密码服务管理平台的数据加解密服务（HMAC-SM3 算法）实现日志的完整性保护。

8.6.4.3.3.1.4 重要可执行程序完整性和真实性

应用服务器中所有重要程序或文件在生成时调用密码服务管理平台，计算完整性鉴别码，将重要可执行程序的关键信息及其完整性鉴别码一同存储到数据库系统中；使用或读取这些程序和文件时，通过调用密码服务管理平台计算其完整性鉴别码并进行校验，以保证重要可执行程序的完整性和真实性。

针对堡垒机设备，通过配置具有商用密码认证证书的密码卡，实现重要资源可执行程序完整性和真实性保护。

针对密码类产品（如：服务器密码机、SSL VPN、纵向加密认证网关、密码服务管理平台等），采用经过商用密码认证机构认证合格的产品，具备相应的安全防护能力，满足相应密码应用需求。

8.6.4.3.3.1.5 重要信息资源安全标记完整性

业务系统涉及的服务器、数据库管理系统、堡垒机、密码服务管理平台、SSL VPN、服务器密码机等设备，均不涉及信息资源安全标记需求，本项为不适用项。

8.6.4.3.3.2 远程运维

远程运维的局域网边界防护措施，在生产管理区（III区）通过纵向加密认证网关实现。远程运维场景中，有关广域网通信的网络和通信保护措施详见网络和通信安全部分，相关终端（PC）、SSL VPN、国密堡垒机等设备与本地运维的设备和计算安全要求一致，应用和数据的访问安全措施详见应用和数据安全部分。

8.6.4.3.4 应用和数据安全

8.6.4.3.4.1 身份鉴别

业务系统的身份认证通过账号口令和国密 USB Key 的方式实现双因子认证。密码服务管理平台提供签名验签服务，实现对系统登录用户基于数字签名的身份鉴别功能，确保系统登录用户身份的真实性。

身份鉴别的流程如下：

(1) 系统用户登录业务应用系统，发送登录请求；

(2) 业务系统调用签名验签服务生成随机数作为挑战码；

(3) 签名验签服务生成随机数返回给业务系统，业务系统暂存挑战码；

(4) 业务系统将挑战码返回给用户客户端；

(5) 客户端调用 USB Key 签名接口对挑战码进行签名，并将签名值和用户数字证书发送给业务系统；

(6) 业务应用系统调用签名验签服务验签接口，传入挑战码、签名值和用户的数字证书，请求验签；

(7) 签名验签服务使用 CA 根证书对用户的数字证书进行有效性验证，验证通过之后，提取系统用户公钥，使用公钥验证签名值，返回验证结果给业务应用系统；

(8) 业务应用系统根据验签结果判定系统登录用户是否为真实可靠的用户，是否允许该用户进行登录，身份鉴别流程结束。

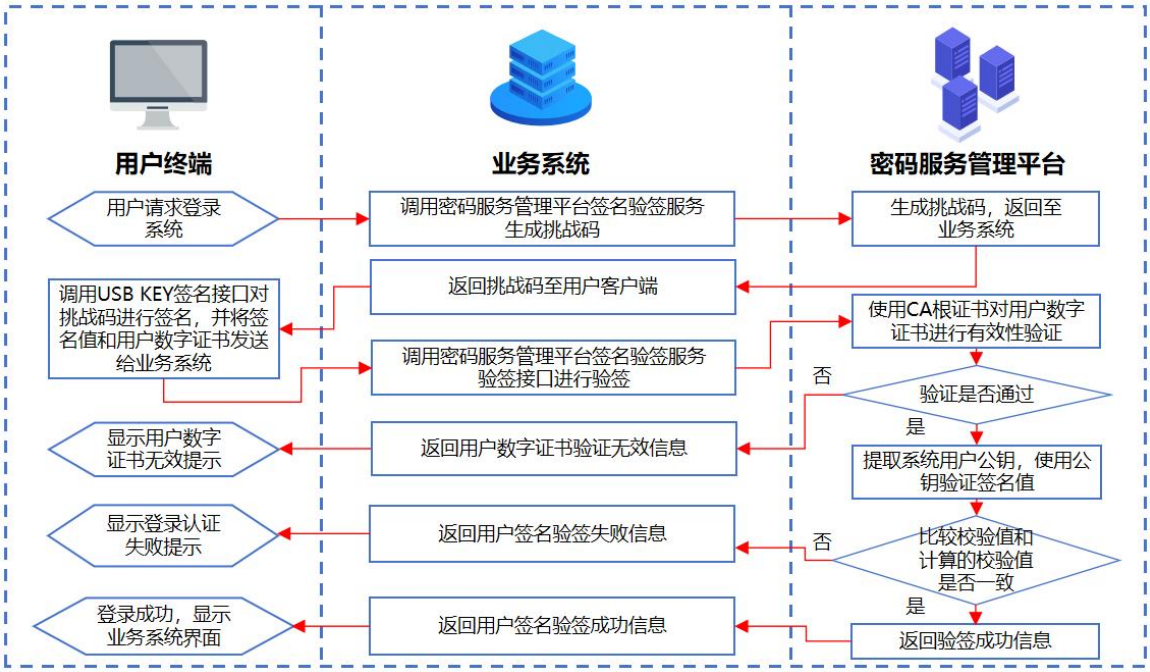

图 8-5 客户端身份鉴别流程

8.6.4.3.4.2 访问控制信息的完整性

业务系统通过调用密码服务管理平台，使用基于 SM4 算法的 MAC、基于 SM3 算法的 HMAC 或基于 SM2 算法的数字签名技术保证业务系统的访问控制信息完整性。

访问控制信息的完整性包括两个部分：系统管理员每次授权完成后，要求对访问控制信息做完整性保护；业务用户每次登录时，要求验证访问控制信息的完整性。

(1) 对访问控制信息进行完整性计算

系统管理员每次授权完成，系统自动调用密码服务管理平台 API 接口，生成完整性鉴别码，并将访问控制列表及其完整性鉴别码同时存储，保证其完整性。

访问控制信息的完整性保护工作流程如下：

1．系统管理员打开系统的授权模块；

2．系统管理员进行授权，并保存；

3．业务系统存储访问控制信息；

4．业务系统将调用密码服务管理平台接口；

5．密码服务管理平台获取访问控制信息，计算访问控制信息生成完整性鉴别码；

6．业务系统保存完整性鉴别码和访问控制信息。

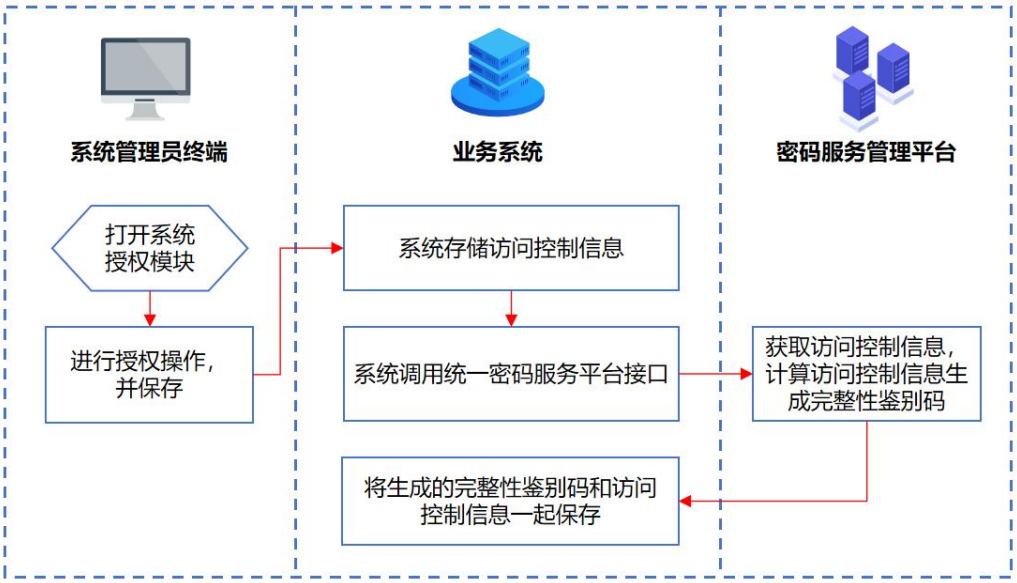

图 8-6 访问控制信息数字签名流程图

(2) 验证访问控制信息的完整性鉴别码

业务用户登录时，业务系统自动调用密码服务管理平台，基于 SM4 算法的 MAC、基于 SM3 算法的 HMAC 或基于 SM2 算法的数字签名技术，验证访问控制信息的完整性，及时发现篡改行为。

访问控制信息的完整性保护工作流程如下：

1．用户/平台管理员通过身份认证；

2．业务系统提取当前访问控制信息和完整性鉴别码；

3．业务系统将调用密码服务管理平台接口；

4．密码服务管理平台获取访问控制信息，计算访问控制信息生成完整性鉴别码；

5．业务系统保存完整性鉴别码和访问控制信息；

6．业务系统比较当前访问控制信息的完整性鉴别码与计算结果是否一致；

7．如果两个值一致，说明访问控制信息未被篡改，业务系统根据用户权限信息在终端显示应用系统的内容；

8．如果两个值不一致，说明访问控制信息已经被篡改，业务系统通知系统管理员处理，并在终端提示系统故障。

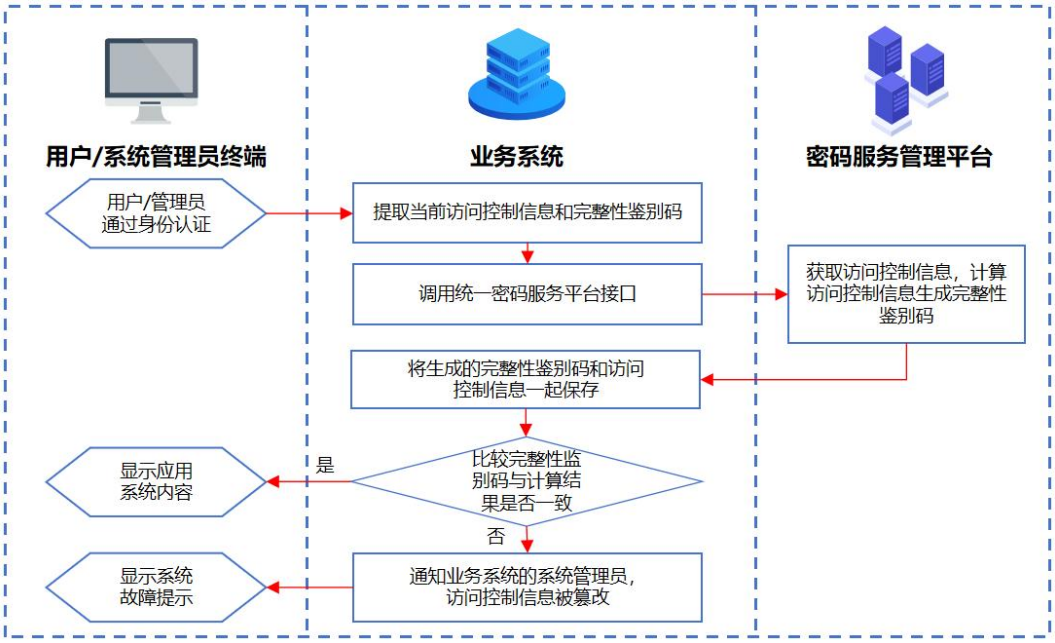

图 8-7 验证访问控制信息数字签名流程图

8.6.4.3.4.3 重要信息资源安全标记完整性

业务系统自身不涉及敏感信息资源，未对信息资源设定安全标记，因此本密码应用方案不涉及此部分内容，此项指标不适用。

8.6.4.3.4.4 重要数据传输的机密性和完整性

业务系统调用密码服务管理平台，对传输中的重要数据进行加密保护，且加密密钥不应以明文形式出现在密码产品外（公钥除外），因此采用数字信封技术实现重要数据的机密性保护，具体地，使用 SM4 算法的对称密钥 K 将数据进行机密性保护，同时使

用非对称密钥对，将对称密钥 K 进行加密，实现数据和密钥的安全传输。同时，采用基于 SM2 算法的数字签名技术实现重要数据的完整性保护。

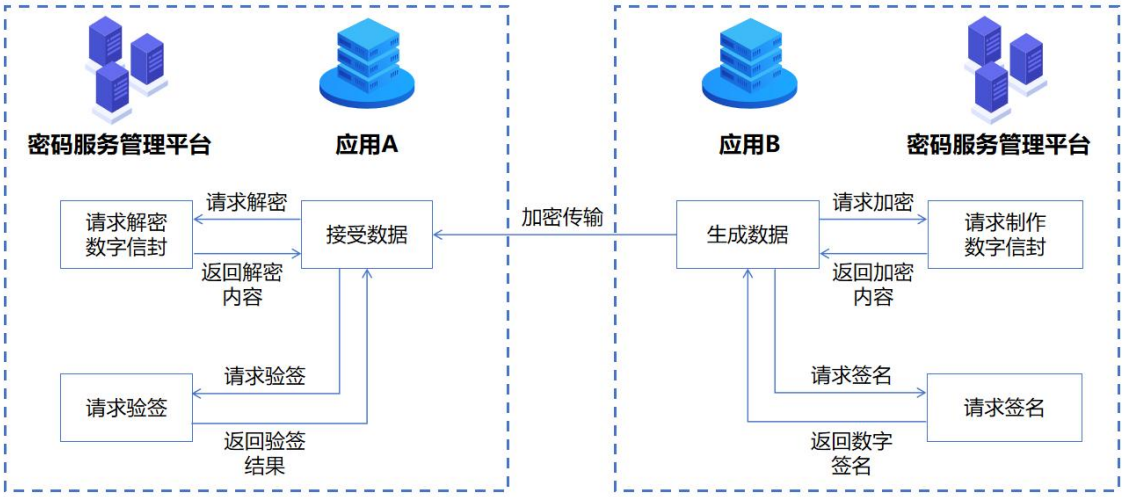

图 8-8 重要数据传输的机密性和完整性流程图

8.6.4.3.4.5 重要数据存储的机密性

业务系统通过调用密码服务管理平台，使用 SM4 算法对业务系统中的鉴别数据、重要业务数据、重要审计及日志数据进行加密存储。

存储的机密性保护包括两个部分：数据录入时，要求使用 SM4 对称密码算法，对重要数据进行加密，防止相关信息泄露；访问读取时，要求使用 SM4 对称密码算法，对重要数据进行解密。

(1) 对重要数据进行加密存储

数据录入人员录入重要数据时，系统调用密码服务管理平台接口，使用 SM4 对称密码算法，对录入的重要数据进行加密。

录入重要数据的加密存储工作流程如下：

1．用户向业务系统输入重要数据后，并提交；

2．业务系统获取录入的重要数据，调用密码服务管理平台接口对数据进行加密；

3．密码服务管理平台使用业务系统的对称密钥，对数据明文生成消息鉴别码，并对数据明文加密得到密文；

4．业务系统存储数据密文和消息鉴别码；

5．用户终端显示存储成功。

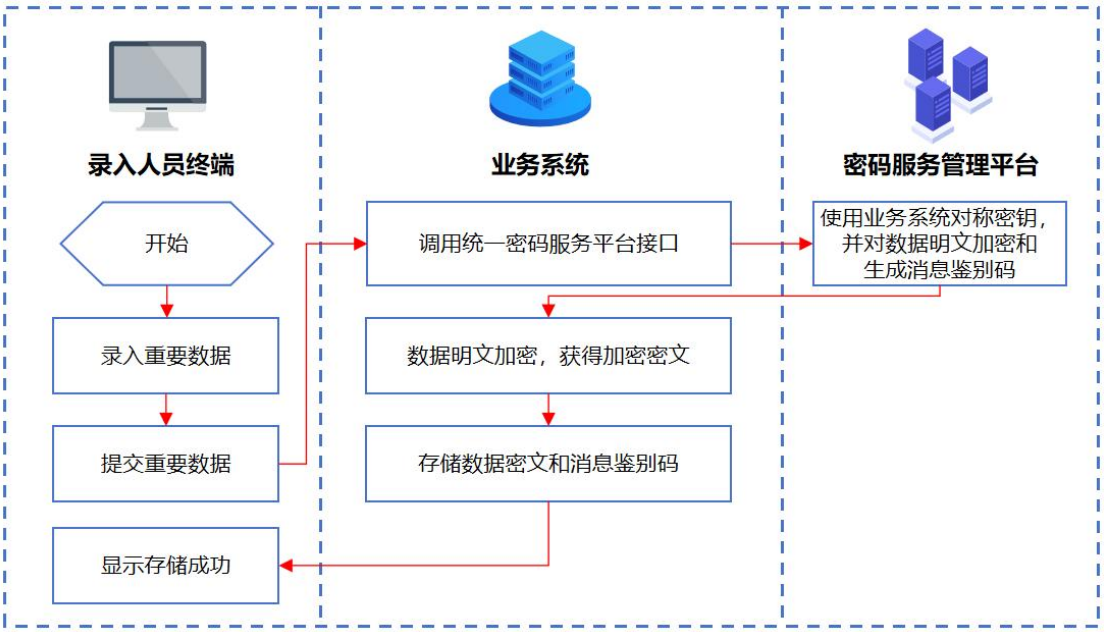

图 8-9 重要数据进行加密存储流程图

(2) 对重要数据进行解密访问

访问业务系统中的加密重要数据时，系统自动调用密码服务管理平台，使用 SM4 对称密码算法，对加密的重要数据进行解密。

访问加密存储的重要数据的解密流程如下：

1．访问人员点击已加密存储的重要数据页面；

2．业务系统将重要数据的密文提交至密码服务管理平台，请求解密；

3．密码服务管理平台使用业务系统的数据加密密钥，解密重要数据的密文；

4．业务系统获得重要数据的明文，向终端展现数据。

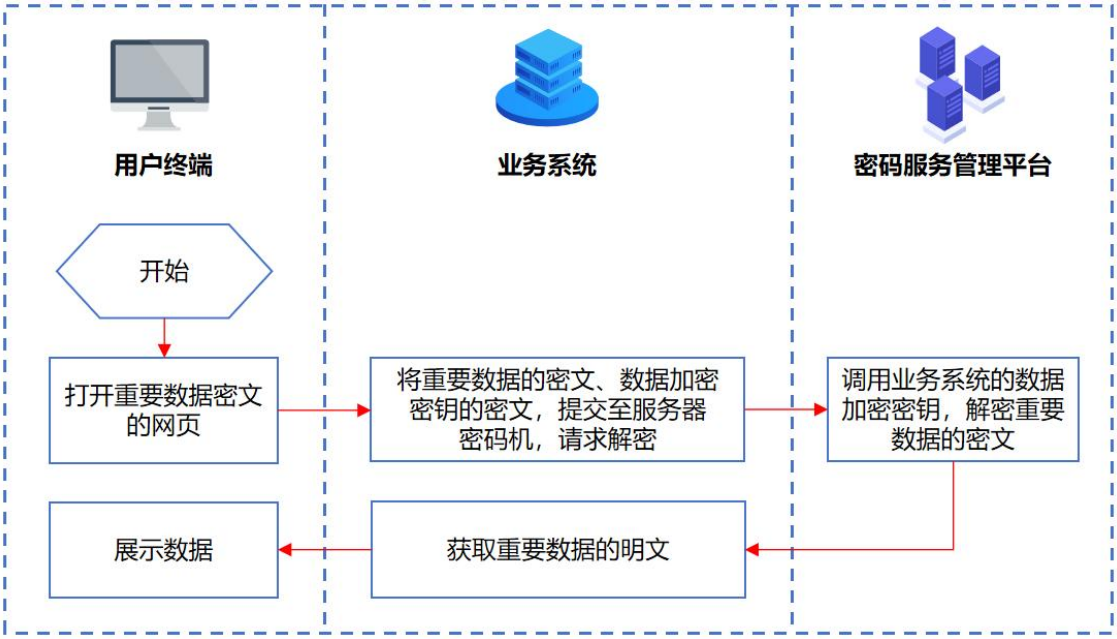

图 8-10 重要数据进行解密访问流程图

8.6.4.3.4.6 重要数据存储的完整性

业务系统通过调用密码服务管理平台，采用基于 SM4 算法的 MAC、基于 SM3 算法的 HMAC 或基于 SM2 算法的数字签名技术对鉴别数据、重要业务数据、重要审计及日志数据存储进行完整性防护。

(1) 对重要数据关键信息进行完整性计算

业务系统发布重要信息时，调用密码服务管理平台，对重要数据计算完整性鉴别码，及时防范可能的篡改行为。

对系统重要数据关键信息的完整性鉴别码计算流程如下：

1．业务系统将重要数据的关键信息，提交到密码服务管理平台，请求计算完整性鉴别码；

2．密码服务管理平台使用业务系统的密钥，对业务系统提交的信息计算完整性鉴别码，并返回给业务系统；

3．业务系统将重要数据的关键信息及其完整性鉴别码一同存储到数据库系统中。

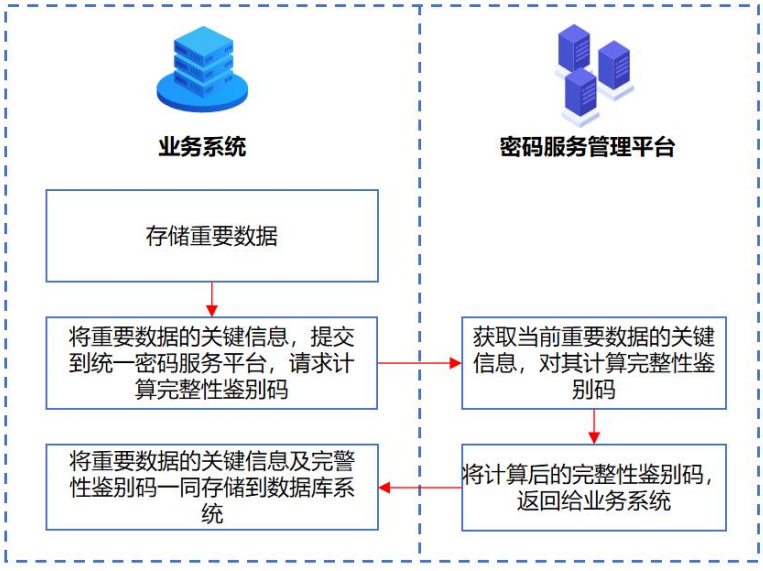

图 8-11 重要数据关键信息完整性计算流程图

(2) 验证重要数据关键信息的完整性鉴别码

用户每次访问重要数据时，业务系统自动调用密码服务管理平台，验证重要数据的完整性，及时发现篡改行为。

验证重要数据相关关键信息的完整性鉴别码流程如下：

1．用户访问业务系统已发布的重要信息；

2．业务系统提取当前重要数据的关键信息及关键信息的校验值；

3．业务系统将重要数据的相关关键信息，提交到密码服务管理平台，请求计算完整性鉴别码；

4．密码服务管理平台使用业务系统的密钥，对业务系统提交的信息计算完整性鉴别码，并返回给业务系统；

5．业务系统比较存储的校验值和计算的校验值；

6．如果两个校验值一致，说明当前重要数据未被篡改，业务系统根据用户需要推送重要数据，在终端显示应用系统的内容；

7．如果两个校验值不一致，说明当前重要数据已经被篡改，业务系统通知平台管理人员处理，并在终端提示系统故障。

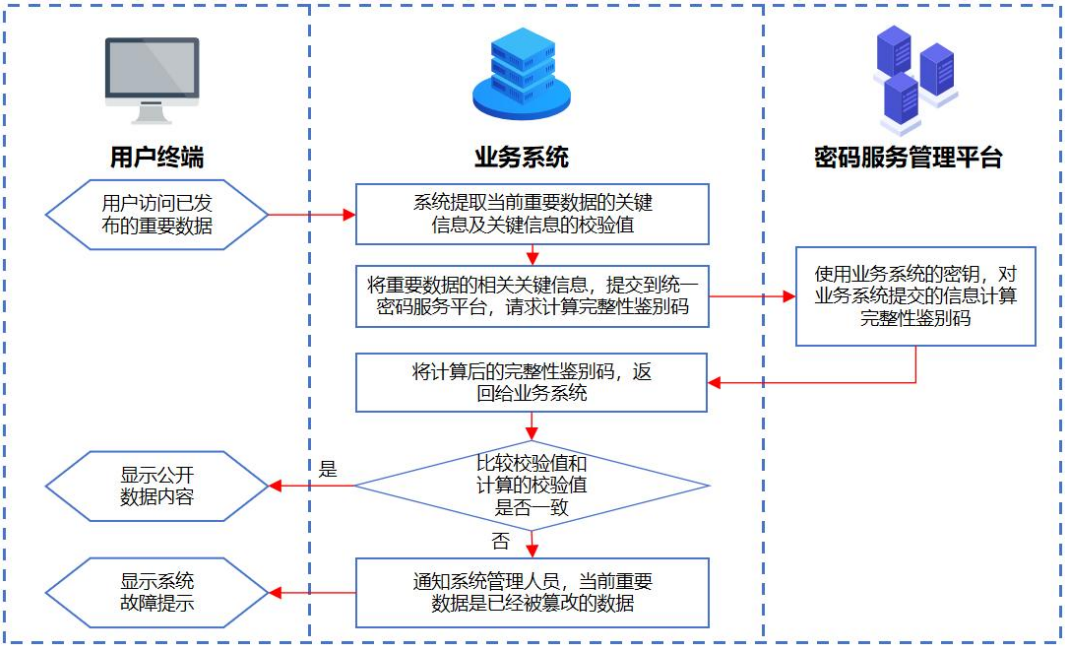

图 8-12 重要数据关键信息完整性鉴别码验证流程图

8.6.4.3.4.7 不可否认性保护

业务系统中不涉及法律责任认定类应用场景，无不可否认性保护的密码应用需求，本项为不适用项。

8.6.4.4 密码服务管理平台要求

密码服务管理平台主要包含密码运算资源池、密码服务层以及管理平台。密码运算资源池为密码服务层提供基础的密钥管理和密码运算服务，密码服务层统一为业务应用提供密码服务；平台管理员可通过管理平台实现用户管理、密码运算资源和密码服务管理等功能。同时，密码服务管理平台对外提供密码功能接口，可为业务或平台应用实现

密码技术的接入。密码服务管理平台及密码应用方案应充分考虑异常处理机制，密码服务管理平台自身出现问题时，对于计量自动化主站系统的核心业务，应优先保障业务系统的正常运行。

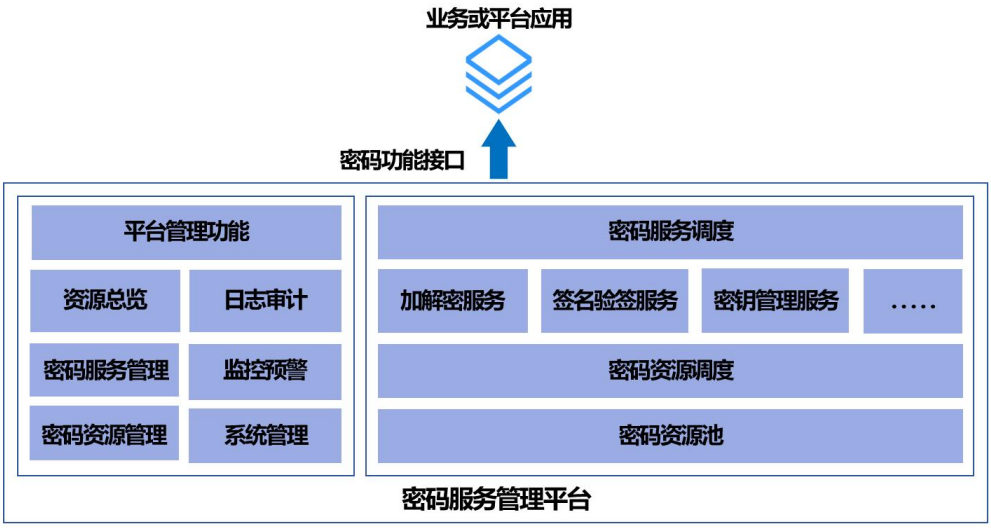

图 8-13 密码服务管理平台功能架构图

8.6.4.4.1 功能要求

8.6.4.4.1.1 平台管理功能

(1) 资源总览

密码服务管理平台可提供密码运算资源使用情况展示、密码服务使用情况展示、接入应用数情况展示、可视化平台展示等功能。

(2) 密码服务管理

支持为指定用户开通指定类型的密码服务；支持密码服务的配置管理、详情查看、升级扩容、关闭释放及重启、备份及恢复等功能。

(3) 密码资源管理

支持用户对密码资源的管理，主要包括密码资源的配置管理、监控查看、开通及删除、关闭释放及重启等功能；支持用户对所属虚拟密码资源分组管理，包括分组的新增、编辑、删除等操作。

(4) 日志审计

提供用户操作及平台运行日志的收集、存储和分析功能，实时监控与分析各种事件和行为的日志记录；支持日志审计功能，可针对用户操作时间、操作人、操作名称、操作结果等日志信息进行审核审计；支持日志外发功能。

(5) 监控预警

支持对密码运算资源的运行状态进行监控，主要监控内容包括 CPU 使用率、内存使用率和连接数等；支持对密码服务整体情况进行监控，如密码服务的 TPS、平均响应值及当天的业务统计监控等；支持异常告警功能。

(6) 系统管理

密码服务管理平台应提供用户管理、权限配置、身份认证、升级维护等系统管理功能。

8.6.4.4.1.2 密码服务调度

密码服务调度实现应用系统和云计算平台接入密码服务的接入和调度管理，包括服务接入认证、服务路由管理、服务协议解析、服务状态检测、服务分发调度功能。

8.6.4.4.1.3 密码服务能力

密码服务管理平台应提供但不限于数据加解密、签名验签及密钥管理等密码服务。

(1) 加解密服务

密码服务管理平台应提供数据的存储加解密服务、传输加解密服务。业务系统进行重要数据的存储时，调用存储加密服务完成数据的加密，使用数据时调用解密服务进行解密；对于跨区数据传输，或者同安全区不同业务系统间的数据传输，发送方对重要数据部分调用传输加密服务进行加密，接收方收到后调用传输解密服务进行解密。

传输数据加解密服务：支持对称算法的传输数据或文件加密、解密服务，支持使用公钥加密会话密钥、会话密钥加密数据的方式对传输数据或文件进行加密。

存储数据加解密服务：支持基于对称算法、散列算法对结构化数据或文件的安全存储进行加密和解密。

密钥申请服务：支持对称密钥、非对称密钥的申请服务，申请对称密钥时，支持公钥加密输出密文或采用数字信封的方式加密输出。

(2) 签名验签服务

签名验签服务应支持密钥管理、证书管理等能力，可为业务系统提供安全的应用层密码服务，有效解决业务系统中伪造、抵赖、冒充和篡改等问题，保证关键业务应用交易过程的机密性、信息完整性、不可否认性和事后追溯性，保障信息系统的安全。

密码服务管理平台可对外提供密码功能接口，接口服务包含签名、验签、数字信封的编制和解封、公钥加密、私钥解密等接口服务。

(3) 密钥管理服务

密钥管理应包含对称密钥管理和非对称密钥管理，支持密钥的生成、存储、备份、恢复、销毁、归档等密钥生命周期管理，应具备灵活性和可扩展性，能够适应不同的算法和标准，同时保证密钥的安全性和合规性。对于密钥的操作，应记录密钥操作日志，包含操作人、操作时间、操作类型、当前密钥值等信息。

8.6.4.4.1.4 密码资源调度

密码服务管理平台支持提供但不限于设备分组管理、设备配置管理、调度策略管理、设备状态监测以及设备负载调度等密码运算资源调度功能。

设备分组管理：应支持根据业务功能要求、性能要求、指令集和型号等进行硬件密码设备使用的分组，同一分组内的设备密钥信息保持一致，系统在同一组中的多台设备进行负载均衡访问。

设备配置管理：应提供对设备的增加、删除、修改设备地址、端口、启用状态等信息的配置和管理，每个设备应具有唯一的标识符，以便进行设备管理和身份识别。

调度策略管理：根据设备的分组信息，为设备的调用创建逻辑分组并设置调度策略。支持当密码接口调用出现会话错误时主动重建会话并重新执行接口调用。支持重建会话失败执行密码机连接异常告警信息的推送，并从同组内其他密码设备获取可用会话重新执行接口调用。

设备状态检测：支持通过建立会话、检测接口调用的方式，定时检测接入的设备服务可用性，当检测到设备网络连接异常或者服务状态异常时，应记录设备异常信息并通过外部接口发送至监控数据采集服务。

设备负载调度：支持通过密码设备分组负载调度密码设备。支持通过设备检测，对状态异常的密码设备主动下线，已下线的密码设备暂时从设备组动态移出，安全服务在设备调度时使用其他密码设备完成密码运算调用，当密码设备状态检测正常时，重新上线该设备。密码机下线时，应记录告警事件信息并通过接口向监控数据采集服务发送告警信息。

8.6.4.4.2 性能要求

项目	性能要求
管理平台	支持管理密码机（物理密码机、虚拟密码机）数量≧100 应用数≧100 管理页面操作响应时间< 3 秒 单线程或单进程调用接口服务单笔响应时间<10 毫秒

项目	性能要求
	服务调用并发用户数≧500 个
签名验签服务	SM2 签名≧8000 次/秒 SM2 验签≧8000 次/秒
数据加解密服务	SM4 加解密≧10000 次/秒 SM2 加密≧8000 次/秒 SM2 解密≧8000 次/秒
密钥管理服务	密钥存储数量≧10 万条 创建对称密钥≧100TPS 创建非对称密钥≧50TPS

8.6.4.4.3 安全性要求

(1) 管理平台操作员应采用双因子身份认证的登录方式，保证用户认证安全；

(2) 管理平台的关键程序、文件应实现完整性校验，保证程序运行的安全性；

(3) 管理平台的密钥应采用密文存储，由存储在密码机的主密钥加密保护，保证密钥安全。

8.6.4.4.4 稳定性要求

(1) 密码服务管理模块应能支持 7×24 小时稳定运行。

(2) 密码服务管理平台应具备高可用能力，出现组件及平台管控自身故障时，不影响现有业务系统运行。

8.6.4.4.5 可靠性要求

(1) 密码服务管理模块应能够正确的执行密码相关的功能和服务，应能够处理各种可能的错误和故障，包括某个服务器故障、某台密码机故障等，确保密码服务的连续性和一致性。

(2) 密码服务管理模块应具备服务逃生模式。在服务层，当所有密码设备均不可用时，应能通过人工或自动的方式，切换成本地模式，通过软算法完成密码服务运算；在接口层，当所有密码服务均不可用时，应能通过人工或自动的方式，切换成本地模式，通过软算法完成密码接口功能运算。

8.6.4.5 密钥管理

本系统所使用的密钥统一由服务器密码机硬件生成，使用密码服务管理平台进行密钥的密文存储。本系统所使用的密钥根据其性质可分为：设备主密钥、应用主密钥、业务密钥（包括对称密钥和非对称密钥）。设备主密钥存放在服务器密码机中，应用主密钥由设备主密钥加密以密文形式存在密码服务平台中，业务密钥（包括对称密钥和非对

称密钥，其中对称密钥含存储及传输机密性密钥、存储及传输完整性密钥、设备主密钥、应用主密钥，非对称密钥含管理用户签名私钥、管理用户验签公钥、SSL 签名私钥、SSL 验签公钥、SSL 加密私钥、SSL 加密公钥）由应用主密钥加密以密文形式存在密码服务平台的密钥管理服务中。

8.6.4.5.1 对称密钥

对称密钥管理应支持国密 SM4 算法。包括密钥的生成、存储、备份、恢复、销毁、归档等密钥生命周期管理，应具备灵活性和可扩展性，能够适应不同算法和标准的要求，同时保证密钥的安全性和合规性。对于对称密钥的操作，应记录对称密钥操作日志，对称密钥操作日志应包含操作人、操作时间、操作类型、当前密钥值等信息。

8.6.4.5.1.1 密钥生成与分类

采用密码设备随机生成 SM4 算法的对称密钥值，确保密钥的安全性和可靠性。

8.6.4.5.1.2 密钥安全存储

对称密钥值以密文方式进行存储，同时保存对称密钥的校验值，用于验证密钥对正确性。密文采用多级加密方式，自上而下逐层保护，以密文的形式存储在数据库或文件，以防止未授权人员访问和窃取密钥。

8.6.4.5.1.3 密钥备份与恢复

对指定密钥进行手动备份时，可同时备份一个或多个密钥，备份的密钥以密文形式存储在本地文件，对备份的内容做完整性校验并将校验值保存在备份文件。

对备份密钥进行恢复时，从备份的密钥文件里面恢复密钥值，执行密钥恢复时，系统应通过检查数据的完整性，以防止备份的内容被篡改。

8.6.4.5.1.4 密钥的归档

支持原始密钥的归档管理，归档后的密钥设置归档状态，保证归档的密钥安全性和正确性，并可以在需要时进行访问。

8.6.4.5.1.5 密钥的销毁

支持对原始密钥进行销毁，并根据情况重新生成密钥，完成密钥更换。密钥进行销毁时，应当删除所有密钥副本，以确保密钥无法恢复或重建。

8.6.4.5.2 对称密钥全生命周期

密钥名称	用途	生成	存储	分发	导入导出	使用	更新	备份和恢复	归档	销毁
存 储	重 要	服 务	由应	不涉	通过 USB Ke	在 服	根据安	通过 USB Ke	根	根 据

密钥名称	用途	生成	存储	分发	导入导出	使用	更新	备份和恢复	归档	销毁
及传输机密性密钥	数据输存过中密解运及储程加及密算	器密机生码中成	用主钥密加密，以密形存在钥理务密管服中	及	y保护式用钥导的方应密密或由主密加出入	务器码中现据解运密机实数加密算	全管理策略定期更新	y保护式用钥进的方应密备恢复由主密加行和	据安全策略在密钥更新过渡期内由密钥管理服务归档	安全略密管服和务密机销策在钥理务服器码中毁
存储传完性及输整密钥	重要据输存过中数传及储程HMAC-SM3运日算、志、权限信息的HMAC-SM3运算	服务密机器码生成	应主钥由用密加密，以密形存在钥理务密管服中	不涉及	通过USB Key保护式用钥导的方应密密或由主密加出入	服器码中现整运在务密机实完性算	根据安全管理策略定期更新	通过USB Key保护式用钥进的方应密备恢复由主密加行和	不涉及	据全略服器码中根安策在务密机销毁
备密设主钥	服务密机器码主密	服务密机器码机生成	储服器码存在务密	不涉及	不涉及	服器码中在务密机	不涉及	通过设密主备份备钥USB Key对	不涉及	据全略服根安策在

密钥名称	用途	生成	存储	分发	导入导出	使用	更新	备份和恢复	归档	销毁
	钥，用于保护应用主密钥		机中			实现运算		服务器密码机进行备份和恢复		务器密码机中销毁
应用主密钥	密码服务平台主密钥，用户保护业务密钥（对称密钥与非对称密钥）	服务器密码机生成	以密文形式存储在密码服务平台中	不涉及	应用主密钥密文（设备主密钥加密）可通过备份数据库、密钥文件的方式导入与导出	在服务器密码机中实现运算	不涉及	应用主密钥密文（设备主密钥加密）可通过备份数据库、密钥文件的方式实现备份与恢复	不涉及	根据安全策略在密码服务平台服务器密码机中销毁

8.6.4.5.3 非对称密钥

非对称密钥管理支持国密 SM2 算法。包括密钥的生成、存储、备份、恢复、销毁、归档等密钥生命周期管理，应具备灵活性和可扩展性，同时保证密钥的安全性和合规性。对于非对称密钥的操作，应记录密钥操作日志，密钥操作日志应包含操作人、操作时间、操作类型、当前密钥值等信息。

8.6.4.5.3.1 密钥生成与分类

采用密码设备随机生成 SM2 算法的非对称密钥值，确保密钥的安全性和可靠性。

8.6.4.5.3.2 密钥安全存储

非对称密钥私钥以密文方式进行存储，同时保存公钥明文，用于验证密钥对的正确性。私钥密文应采用多级加密方式，自上而下逐层保护，以密文的形式存储在数据库或文件，以防止未授权人员访问和窃取密钥。

8.6.4.5.3.3 密钥备份与恢复

对指定密钥进行手动备份时，同时备份一个或多个密钥，备份的密钥以密文形式存储在本地文件，对备份的内容做完整性校验并将校验值保存在备份文件。

对备份密钥进行恢复时，从备份的密钥文件里面恢复密钥值，执行密钥恢复时，系统应通过检查数据的完整性，以防止备份的内容被篡改。

8.6.4.5.3.4 密钥的归档

支持原始密钥的归档管理，归档后的密钥设置归档状态，保证归档的密钥安全性和正确性，并可以在需要时进行访问。

8.6.4.5.3.5 密钥的销毁

支持对原始密钥进行销毁，并根据情况重新生成密钥，完成密钥更换。密钥进行销毁时，应当删除所有密钥副本，以确保密钥无法恢复或重建。

8.6.4.5.4 非对称密钥全生命周期

密钥名称	用途	生成	存储	分发	导入导出	使用	更新	备份和恢复	归档	销毁
管理用户签名私钥	管理员登录时通过USB Key对挑战码进行签名	USB Key中生成	以密文形式存放在USB Key中	不涉及	无法导入导出	实现数据的签名操作	证书到期或时作更新	不涉及	不涉及	证书到期或时作废销毁
管理用户验签公钥	应用系统对USB Key签名值进行验证	USB Key中生成	以明文形式存储在证书中	不涉及	随证书导入导出	实现数据签名的验操作	证书到期或时作更新	不涉及	不涉及	证书到期或时作废销毁
SSL签名私钥	通信过程中通过私钥签名证明服务端身份	在SSL VPN中生成	以密文形式存储在密码卡中	不涉及	支持导入，以密文的方式导出	在SSL安全网关中进行签名运算	证书到期或时作更新	以密文形式加密在硬件设备本地备份，支持密钥	不涉及	SSL证书废更时同步销毁

密钥名称	用途	生成	存储	分发	导入导出	使用	更新	备份和恢复	归档	销毁
								恢复		
SSL验签公钥	通信过程中通过公钥验证服务端身份	在SSL VPN中生成	在SSL签名证书中存储	随证书分发	随证书导入导出	在SSL客户端（浏览器）中进行验签运算	证书到期或时作更新	随证书备份和恢复	不涉及	SSL签名证书废或更新时同步销毁
SSL加密私钥	SSL协商过程中，服务端解密客户端传上的密钥因子	由第三方CA机构生成	以密文形式存储在密码卡中	不涉及	支持导入，以密文的方式导出	在SSL安全网关中解密运算	证书到期或时作更新	以加密文件式备份，支持密钥恢复	不涉及	SSL加密证书废或更新时同步销毁
SSL加密公钥	SSL协商过程中，客户端加密上的密钥因子要传	由第三方CA机构生成	在SSL加密证书中存储	随证书分发	随证书导入导出	在SSL客户端（浏览器）中进行加密运算	证书到期或时作更新	随证书备份和恢复	不涉及	SSL加密证书废或更新时同步销毁

8.6.5 商密应用合规自检要求

本项目应符合《GB/T 39786-2021 信息安全技术 信息系统密码应用基本要求》第三级密码应用基本要求。

要求投标方根据下述自检要求进行前期自查，填写密码应用合规要求自检表。

在国家商用密码应用测评过程中，中标方应负责内容包括但不限于网络和通信安全、设备和计算安全以及密码服务管理平台层面的密码应用，物理和环境安全、应用和数据安全层面密码应用由机房工程及主站应用功能建设开发厂家负责，中标方需与其他相关

方紧密配合，共同完成系统的密码应用安全建设，保证本项目的国家商用密码应用测评分值达到合格分及以上且密码应用无高风险。

密码应用合规要求自检表

指标要求	密码技术应用点	采取措施	标准符合性
物理和环境安全	身份鉴别		
	电子门禁记录数据完整性		
	密码模块实现		
网络和通信安全	身份鉴别		
	访问控制信息完整性		
	通信数据完整性		
	通信数据机密性		
	集中管理通道安全		
	密码模块实现		
设备和计算安全	身份鉴别		
	远程管理身份鉴别信息机密性		
	敏感标记的完整性		
	日志记录完整性		
	访问控制信息完整性		
	重要程序或文件完整性		
	密码模块实现		
应用和数据安全	身份鉴别		
	访问控制信息和敏感标记完整性		
	数据传输机密性		
	数据传输完整性		
	数据存储机密性		
	数据存储完整性		
	日志记录完整性		
	重要应用程序的加载和卸载		
	抗抵赖（四级）		
	密码模块实现		

8.7 数据安全要求

8.7.1 数据备份恢复

支持通过云服务器快照，数据库备份等功能实现业务数据的备份恢复，加强数据可靠性与业务连续性的保障。提供异地数据备份功能，利用通信网络将重要数据备份至异地备份场地。

8.7.2 数据脱敏

使用静态脱敏组件技术，识别数据中的敏感信息，通过高效的脱敏算法对数据进行屏蔽、遮盖、变形处理，实现将敏感数据转化为虚构数据，保证脱敏后数据的业务关联完整性，避免因数据外发造成敏感信息泄露等安全事件。支持针对敏感数据的静态脱敏，可根据用户、应用的权限不同，动态调整脱敏算法，满足不同应用场景需求。静态脱敏主要是通过复制一份原始数据，并将需要脱敏的字段进行脱敏处理后提供使用。

应提供数据脱敏组件接口给主站应用功能建设开发厂家调用，配合主站应用功能建设厂家实现主站系统的数据脱敏功能。

8.7.3 数据水印

计量自动化主站在数据共享、数据交换、追踪溯源方面通过数据水印组件，采用数据水印措施，对数据的使用、访问路径进行追踪，降低敏感信息泄露风险。

数据库水印、文档水印方面，使用数据水印组件技术，将水印信息隐藏在数据中，实现对数据进行追踪，一旦发生数据泄露可追溯定责。

屏幕水印方面，使用明水印、隐水印、透明水印等技术，在数据库或相关文档交换、静态页面展示及动态页面生成过程中嵌入数据水印，实现在数据泄露发生后，对泄露数据进行水印信息的提取，查询到数据的分发源、分发对象、分发日期等相关信息。

应提供数据水印组件接口给给主站应用功能建设开发厂家调用，配合主站应用功能建设厂家实现主站系统的数据水印功能。

8.7.4 应用开发数据安全要求

应用开发、测试、发布、运维方面，为保障程序包（源码包）和开发文档安全不至于泄露、滥用或组织的名誉损害等不良影响事件发生，要求厂家在应用开发、测试、发布、运维等环节，满足以下应用开发数据安全管理要求，包括通用数据安全、运维数据安全、应用开发数据安全：

8.7.4.1 通用数据安全要求

(1) 严禁使用明文保存账号密码信息。

(2) 严禁越权使用他人账号密码。

(3) 严禁使用互联网网盘（如百度网盘、阿里网盘等）、公共信息服务平台（如百度文库等）存储、共享公司敏感信息。

(4) 严禁使用公共社交媒体工具（如微博、抖音等）传播公司敏感信息。

(5) 严禁使用拍摄设备（如手机、数码相机等）拍摄并传播公司敏感信息。

(6) 严禁随意摆放、丢弃含有公司敏感信息的纸质材料。

(7) 严禁在非涉密计算机处理公司涉密信息。

(8) 严禁窃取或者以其他非法方式获取数据。

(9) 严禁未经加密（SHA2、RSA 等）或者脱敏传输敏感数据。

(10) 严禁利用公司数据进行非法经济活动。

(11) 严禁未授权数据出境活动。

(12) 严禁参与暗网、红客联盟等社会网络活动。

8.7.4.2 运维数据安全要求

(1) 严禁在运维设备上存储公司敏感信息。

(2) 严禁运维设备同时连接内外网，传输数据。

(3) 严禁未经授权设立运维账号或者交叉使用、混用运维账号。

(4) 严禁未经授权访问、使用、修改、删除数据库、配置文件等数据。

(5) 严禁未经授权更改网络及服务器等设备的各项参数。

(6) 严禁未经授权将运维数据泄露给第三方。

(7) 严禁将生产数据直接导出，必须通过充分的脱敏、加密后，在专人陪护下导出使用并及时销毁。

(8) 严禁通过 VPN、远控工具（如 teamviewer、向日葵等）等方式进行远程运维。

(9) 严禁未落实保密措施的情况下，使用外部技术服务人员开展作业。

8.7.4.3 应用开发数据安全要求

(1) 严禁未经编译及加密直接导出源代码使用。

(2) 严禁未经脱敏将生产数据直接导入测试环境或者开发测试使用。

(3) 严禁未经审批流程直接开放业务 API 接口或者调用 API 权限。

(4) 严禁将各类开发、测试、演示系统及生产管理界面向互联网开放。

(5) 严禁有意破坏或者窃取源代码。

(6) 严禁对外泄漏开发内容、程序及数据结构。

(7) 严禁使用不安全的第三方组件。

(8) 严禁开发恶意程序。

(9) 严禁擅自搭建应用。

8.8 电力监控系统网络安全要求

南方电网电力监控系统及其网络原则上划分为生产控制大区和管理信息大区。生产控制大区原则上划分为控制区（安全区 I）和非控制区（安全区 II）。管理信息大区原则上划分为生产管理区（安全区 III）和信息内网区（安全区 IV）和信息外网（安全区 V）。

(1) 不允许把应当属于高安全等级区域的业务系统或其功能模块迁移到低安全等级区域；但允许把属于低安全等级区域的业务系统或其功能模块放置于高安全等级区域。

(2) 横向网络边界网络安全防护

1．控制区与非控制区之间的访问控制策略只允许控制区系统主动与非控制区系统建立连接，不允许从非控制区反向访问控制区系统。

2．严禁 E-mail、web、telnet、rlogin、ftp 等高安全风险的通用网络服务和以 B/S 或 C/S 方式的数据库访问穿越专用横向单向安全隔离装置，仅允许纯数据的单向安全传输。

(3) 纵向网络边界网络安全防护

1．在生产控制大区纵向网络边界上，避免使用默认路由，仅开放特定通信端口，禁止开通 ftp、telnet、rlogin、rsh、rcp、http、pop3 等高风险网络服务。

2．生产控制大区系统互联交互的网络通信服务端应部署在低安全区、下级主站或厂站侧，低安全区的业务不允许主动连接高安全区的业务，下级系统不允许主动连接上级系统。

(4) 生产控制大区内部应符合以下要求：

1．禁止生产控制大区内部的 E-mail 服务、telnet、SMB 共享、rlogin、FTP 服务等。

2．禁止控制区内通用的 WEB 服务等。

3．禁止生产控制大区以任何方式连接因特网。

(5) 访问控制措施

1．重要（关键）操作模块支持多次防误确认功能和多角色监督制衡确认功能，重要操作由多个系统管理员确认后方可执行；

2．配置账户操作行为风险控制模块，对于登录异常、操作异常等各类异常行为进行感知和告警；

3．配置账户操作行为审计模块，保存账户的操作记录。

(6) 应用系统安全

1．应用系统具备强制要求管理员账户、用户账户口令定期进行变更功能；

2．严格管理应用权限，制定权限赋予和权限变更的审核、批准、执行流程，依据最小化原则对用户赋予适当的权限，并定期进行权限复核；

3．对应用系统进行数据输入的合法性和参数配置的正确性检验；

4．系统上线运行前对其进行安全性检测以及源代码的漏洞检测；

5．系统软件禁止使用 21、135、137、138、139、445、513、3389 等高危端口进行业务通信或数据同步。

6．安全 II 区若有 WEB 服务，采用支持 HTTPS 的安全 WEB 服务，其 WEB 服务器必须经过安全加固并采用电力调度数字证书对浏览器客户端访问进行身份认证及加密传输。

8.9 安全统一监测要求

建立贵州计量 3.0 安全监测能力，提供基础设备、云计算平台的统一安全监测；提供物理资源和虚拟资源的统一状态监测，边缘集群各个安全区域的监测信息，需要通过物理隔离装置实现监测信息跨安全区传输，最终全部汇总在贵州计量检定中心基地的安全III区。由主站应用功能建设厂家负责，本项目中标方应配合完成接口联调工作，实现安全统一监测。

计量自动化系统分布式平台在贵州安全III区提供各安全分区的网络运行状态、操作系统日志、中间件日志、数据库日志、应用系统日志、安全设备日志、安全管理中心等等本次供应的所有软硬件设备的监测信息，并提供接口实现与主站应用功能建设厂家进行内部数据交互。

主站应用功能建设厂家需将日志汇总收集并长期保存（不少于六个月），并调用密码服务管理平台对日志做完整性保护。并实现手动和自动的完整性验证。由主站应用功能建设厂家进行安全监测相关应用开发，进行安全监测的可视化展示，实现对系统所有

日志的分析、告警、展示。

本项目中标方应配合主站应用功能建设厂家完成接口联调工作。

8.10 项目网络安全增强要求及措施要求

8.10.1 项目网络安全增强要求

增强要求	具体内容
加强系统网络资产摸底排查	重点易被忽略的设备资产类型，确保 100%梳理核实到位，形成完整准确的资产台账清单，结合态势感知实用化工作，做好相关台账录入，确保帐、图、实一致。
网络准入白名单	梳理生产终端、运维终端网络接入 IP 地址、端口及账号白名单，通过网络准入、交换机等设备实行明细的准入管控，具体细化至单个终端。
加强边界和主机安全防护	确保隔离装置无漏洞、缺陷，软件版本为最新。
加强云平台安全防护	全面梳理 VPC、云租户的资源分配及使用情况，释放各类测试资源、闲置资源、临时使用资源等非必要资源，保证最小化运行。
建立项目网络安全台账	在项目实施过程中建立健全计量自动化系统 3.0 网络安全台账，确保系统建设阶段安全防护措施执行到位。

8.10.2 项目网络安全增强措施要求

内容	具体要求	计量 3.0 措施
加强系统网络资产摸底排查	重点易被忽略的设备资产类型，确保 100%梳理核实到位，形成完整准确的资产台账清单，结合态势感知实用化工作，做好相关台账录入，确保帐、图、实一致。	计量自动化系统 3.0 严格落实安全管理制度，形成由安全策略、管理制度、操作规程、记录表单等构成的全面的安全管理制度体系，主站、平台厂家需配合完成网络安全资产摸底排查，结合安全管理中心、态势感知等设备组件，做好系统的资产台账清单。
网络准入白名单	梳理生产终端、运维终端网络接入 IP 地址、端口及账号白名单，通过网络准入、交换机等设备实行明细的准入管控，具体细化至单个终端。	计量自动化系统 3.0 各安全区域配置网络终端接入核查设备进行准入管控，细化白名单策略
加强边界和主机安全防护	全面完成边界隔离装置缺陷整改和软件升级。	计量自动化系统 3.0 各安全区域间边界部署电力专用隔离装置/纵向加密认证网关/边界防火墙设备保障边界安全，平台部署主机安全组件等构建主机安全防护能力。 主站、平台厂家需对相关设备及时进行缺陷整改及软件升级，确保设备不存在缺陷漏洞、软件保持在最新版本。

内容	具体要求	计量 3.0 措施
加强云平台安全防护	全面梳理 VPC、云租户的资源分配及使用情况，释放各类测试资源、闲置资源、临时使用资源等非必要资源，保证最小化运行。	主站、平台厂家需配合完成 VPC、云租户的资源分配及使用情况梳理工作，结合安全管理中心、云平台的运营管理、运维平台等设备组件，做好云平台的安全防护工作，释放各类测试资源、闲置资源、临时使用资源等非必要资源，保证最小化运行。

9 项目进度要求

相关工作进度详见下表，可根据“贵州电网公司计量自动化系统 3.0 建设”项目建设情况及要求，在技术联络会中进行合理调整。

任务安排	完成时间	工作内容/成果
合同签订	中标通知书发出一个月内	合同文件；
		合同谈判纪要；
第一次技术联络会	中标通知书发出两周内	技术方案沟通；
		会议纪要；
设备供货	合同签订三个月内或以建设单位通知为准	设备到货
		实施方案的编制（包括施工图草图）
第二次技术联络会	正式施工前一个月	施工图交底
平台集成实施	机房具备实施条件且设备到货验收后 2 个月内	平台软硬件安装调试
第三次技术联络会	以建设单位通知为准	配合主站应用功能建设厂家安装调试、项目各中标方集成联调沟通
问题消缺	现场验收前	消缺报告
现场验收	合同签订之日 6 个月内，或以建设单位通知为准	现场验收报告
双轨试运行	现场验收后 3 个月	试运行情况报告
单轨运行	项目竣工验收前	运行情况报告
竣工验收	合同签订之日 14 个月内，或以建设单位通知为准	竣工验收报告、竣工草图、竣工决算、其他竣工资料

10 项目实施要求

10.1 实施要求

(1) 本技术规范书中所规定功能，若需要与其他系统互联获取数据的，相关接口必须调试完成，获取的业务数据应完整、准确。为方便对方的系统升级改造，投标方系统对外的接口设计都应满足双通信接口要求，以便对方系统并行运行。接口调试过程中，

投标方应保证与用户及对方单位积极配合，保证调试顺利完成。请投标方确认并明确，与其他系统互联调试是整个项目的重要部分，投标方应积极配合；相关费用应包含在投标报价中。

(2) 中标方应负责所供软件设备的现场安装调试、技术联络、培训、会议等在内的技术服务；其中安装调试工作，除了软件设备本身的安装调试外，还应包含应用系统的图形、模型、报表等的生成工作，以及数据整合工作，相应费用均应包含在总报价中。中标方应积极配合项目建设工作，与监理单位、设计方、其他接口方、测试验收单位积极配合，如因中标方原因或配合不力造成的一切损失，均由中标方负责。

(3) 投标方所供货物应与其他设备厂商（包含通信、自动化产品）所供产品兼容性良好，如因兼容性问题、质量问题、安全问题等等需要设备调换或测试，中标方应积极配合，不得以任何理由拒绝。项目质保期结束前，因兼容性问题、质量问题、安全问题等等产生的设备调换或测试费用由中标方承担。

(4) 投标方应给出完整的建设团队组织结构和人员配置，投标方应保证现场实施、技术服务、后台专家等人员组成的团队为最终中标项目服务。

(5) 中标方在项目实施过程中为保障项目顺利实施所需的任何费用包括但不限于临时用水、用电、仓储、运输及质押金等各类费用均包含在本次的投标报价中。

(6) 中标方必须严格按照贵州电网公司要求的项目进度开展工作，若因中标方原因造成工期拖延，贵州电网公司及相关单位的所有损失均由中标方负责。

10.2 项目管理

中标方与贵州电网公司依据“项目进度要求”章节项目进度要求开展项目建设工作，可在合同谈判及技术联络会阶段对项目进度合理调整。

10.3 会议与联络

10.3.1 技术联络会

(1) 为便于合同的执行、审查和系统设计方案的确定，中标方与贵州电网公司根据需要举行技术联络会，除按合同规定举行的技术联络会外，双方可以根据需要约定对方举行额外的设计联络会。

(2) 技术联络会的时间根据贵州电网公司要求安排进行；地点根据项目需要，由双方约定。

(3) 每次技术联络会招投标双方均签署会议纪要，纪要将视为合同的组成部分。

(4) 技术联络会的贵州电网公司参加人数及天数，根据项目需要及贵州电网公司需求确定。

10.4 试运行要求

(1) 在现场对每台设备及整个系统测试的指标应与技术说明书相一致。如果所有的测试结果显示设备和整个系统均符合技术说明书的要求，即开始设备和整个系统的试运行。

(2) 设备及系统的试运行期根据贵州电网公司要求约定。

(3) 对于考查系统稳定性所做的记录，中标方或贵州电网公司各部门均不允许做任何随意的调整。在此期间，如果任何设备（部件）有故障或系统指标降低，中标方应负责处理并使其满足指标要求。但自设备（部件）恢复正常运行之日起，试运行期将重新开始并延续 1 个月。

(4) 对于任何设备的例行测试显示其未能达到所保证的标准且中标方在首次故障 1 个月内不能修复使其达到所保证的标准，中标方应无条件予以更换并承担由此造成的一切损失。

11 项目验收要求

11.1 总体要求

(1) 中标方按照技术规范要求编制详细的测试验收大纲，并经贵州电网公司、测试单位、监理方、设计方审查确认后作为正式的测试验收依据，共同遵守。

(2) 中标方负责配合系统到货验收，所提供的软件设备需经过点验，设备型号、数量、配置与供货合同一致，设备状况完好，确认无误后，方可由贵州电网公司进行签收。

(3) 中标方负责配合系统集成测试验收。所提供的系统必须经过系统集成测试验收，并且其结果都已经过贵州电网公司、测试单位、监理方、设计方以及系统集成验收测试小组的签字认可后才可由贵州电网公司进行系统集成测试验收报告签字。

(4) 中标方配合贵州电网公司进行现场测试验收，并完成现场验收测试大纲的编制工作。

(5) 中标方配合贵州电网公司进行“贵州电网公司计量自动化系统 3.0 建设”项目竣工验收，并配合完成竣工材料编制。

(6) 如采购的是第三方软件，需出具第三方厂商提供的确认函。

(7) 系统测试与验收划分为三个阶段，即到货验收、系统试运行、项目验收。

11.2 系统到货验收

11.2.1 签收条件

中标方所提供所有设备必须开展到货验收。供货合同中规定的供货范围内的软硬件设备到达贵州电网公司指定的现场，经过贵州电网公司认可并在到货验收报告签字确认后，方可由贵州电网公司进行设备的签收。

11.2.2 验收标准

设备到货验收需满足到货的品牌、型号、数量与配置与订货清单一致性、设备的外观完好性、设备通电自检正常。

11.2.2.1 产品外观检测

(1) 硬件产品检测

1．设备品牌、型号、配置及硬件模块型号、配置应与合同规定的配置清单完全一致。

2．设备外包装应完整，无严重变形，应为设备原包装并应各种标识齐全。

3．设备外观应无划痕、碰伤以及其它明显缺陷。

(2) 软件产品检测

1．产品型号应与合同规定的配置清单完全一致。

2．产品外包装应完整，无严重变形，应为产品原包装并应各种标识齐全。

3．软件介质外观应无划痕、碰伤以及其它明显缺陷。

4．软件内容应可通过计算机识别、无病毒、各功能模块可正常安装。

11.2.2.2 产品随机附件检测

检测方法：双方人员参照随机附件清单清点附件或资料（注：无附件清单的设备可查看附件包外包装是否完整并参考厂商的相关附件说明）。

(1) 随机附件或资料应完整齐全。

(2) 各附件或资料应无损坏或与产品内容不配套现象。

11.2.2.3 产品加电检测

检测方法：给设备接通电源（软件产品则是将介质放入计算机的介质设备），对以下检测内容进行确认。

(1) 网络设备（通过 Console 口连接进行检测）

1．设备应能够正常启动，期间不应有故障报错信息。

2．设备启动自检各项硬件信息，包括内存容量、模块信息、软件版本等，应与合同规定的设备应有配置相符合。

3．设备启动后系统状态指示灯显示应符合设备相关技术要求。

(2) 计算机设备

1．设备应能够正常启动，期间不应有故障报错信息。

2．设备启动自检各项硬件信息，包括 CPU 频率、内存容量、硬盘容量等，应与合同规定的设备应有配置相符合。

3．主机如有预装操作系统，应能够正常运行。

(3) 软件产品

1．介质内容应可通过计算机识别。

2．介质内容应无病毒或其他与合同要求无关的内容。

3．软件产品的各功能模块应可以正常被安装。

4．对各软硬设备配置进行检查确认，进程一览表应对进程名、功能、是否为常驻进程、运行位置等进行表述。

11.2.3 验收报告

设备到货验收结束后，中标方应配合贵州电网公司编写设备到货验收报告，设备到货验收报告应包含以下内容：

(1) 设备到货验收结论

(2) 设备到货清单

11.2.4 验收责任

设备到货验收过程中，如因中标方原因，导致设备数量、型号、配置与供货合同确定的供货清单不一致的，或者设备状况不满足验收标准的，中标方应无条件进行补货、退货、换货等处理，所产生的一切费用由中标方承担。

如因中标方原因不能及时完成到货验收，则由此引起的一切开销及后果由中标方承担。

11.3 现场验收测试（SAT）及试运行

现场验收测试包括：功能现场验收测试、工程量现场验收、施工现场验收，为“贵州电网公司计量自动化系统 3.0 建设”项目正式竣工验收提供相应的材料及依据。

11.3.1 系统现场验收内容

现场验收测试内容严格按照技术规范进行。

11.3.2 测试人员

中标方应派出多名有经验的工程师参加 SAT。

11.3.3 测试责任

(1) 协助进行现场验收测试，提供测试验收需要的条件及工程实施文档。

(2) 在进行 SAT 时，系统的所有测试是在实际数据和通信通道上进行的。在 SAT 完成后 5 天内，双方的代表签署 SAT 验收报告。

(3) SAT 的测试验收大纲由中标方按照贵州电网公司要求编制准备，并在系统 SAT 测试前交给贵州电网公司审查同意。SAT 的测试条件中，包括：

1．系统所有功能及工程安装、调试工作全部完成。

2．最终的 SAT 项目内容将在技术联络会上讨论确定。

(4) 为有利于系统的安装、投运和测试，中标方应派出多名有经验的专家提供技术服务。

(5) 在现场安装、投运及验收过程中，中标方对损坏的设备负责，除非设备的损坏是由于贵州电网公司在未经中标方工程师事先同意的情况下误操作而引起。

11.3.4 系统试运行

在通过现场验收测试后，系统当立即投入试运行。

11.3.4.1 系统试运行内容

系统试运行内容严格按照技术规范进行，系统在正式进入试运行后，应在要求时间范围内连续稳定运行。

11.3.4.2 责任

中标方必须积极配合进行相关的工作，保证系统在试运行期间内稳定运行；如果试运行期间内出现问题，重新计算试运行周期，相关责任由中标方承担。

11.4 项目验收

项目验收时间安排在合同签订之日 14 个月内，或以建设单位通知为准。

11.4.1 验收条件

(1) 现场验收遗留问题已基本解决；试运行期间系统运行稳定、正常，项目建设文件已编制完成；

(2) 试运行期满后，已编制完成“贵州电网公司计量自动化系统 3.0 建设”项目竣工验收申请报告和试运行报告；

(3) 完成项目验收大纲编制。

11.4.2 验收标准

(1) 系统在试运行期间运行稳定可靠，未出现应用服务非人工切换、重要进程非正常终止、崩溃、死机等稳定性问题；

(2) 中标方提交的技术手册、使用手册和维护手册应符合要求，且正确有效；

(3) “贵州电网公司计量自动化系统 3.0 建设”项目竣工验收测试结果满足《计量自动化系统分布式平台基础设施》技术规范书，无工程化问题；

(4) 项目工程清册已汇编装订，系统应急预案及运行维护管理制度已制订实施。

11.4.3 验收报告

“贵州电网公司计量自动化系统 3.0 建设”项目竣工验收结束后，中标方应配合贵州电网公司编写竣工验收报告，竣工验收报告应包含以下内容：

(1) 竣工验收结论；

(2) 竣工验收测试报告；

(3) 竣工验收差异汇总报告（同时作为竣工验收遗留问题备忘录；制造单位应对每一项差异提出解决方法和预计解决时间，限期处理完成）；

(4) 竣工验收设备和文件资料核查报告；

(5) 竣工验收测试大纲。

11.5 验收费用

(1) 投标方应将系统验收等的相关费用作为总标价的一部分。

(2) 在中标方及其它地点举办的验收会等，由中标方负责验收会议费用和贵州电网公司人员的往返交通、当地交通、食宿费用等；在贵州电网公司举办的验收会，由中标方负责所需的验收会议费用和贵州电网公司聘请的验收测试人员、验收专家等的食宿费用等。

(3) 测试与验收包括“贵州电网公司计量自动化系统 3.0 建设”项目到货验收、现场验收、竣工验收等，贵州电网公司参加各项测试验收的人天数由贵州电网公司根据测试验收的具体工作需求确定。

12 售后服务要求

12.1 总体要求

(1) 系统发生故障后，中标方应在 2 小时内作出响应。

(2) 在系统生命周期内，中标方所供第三方软硬件的相关维护、完善由中标方统一负责协调相应的原厂商进行处理。

(3) 中标方应在贵阳设有用户服务中心或维修点，配有专职维修人员，备有充足备品备件，并有完善的用户档案，能及时准确解决所提供设备的故障。

(4) 在质保期满后，中标方仍应满足贵州电网公司对所出现故障的设备进行维修的要求。

(5) 中标方提供售后服务及售后服务的组织情况。

(6) 在系统生命周期内，如果贵州电网公司需要对中标方所供系统进行升级扩容、购买备品备件和质保期后的技术服务等，中标方负责协助完成。

(7) 中标方应承诺：在整个系统运行生命周期内，系统扩容所需的云平台软件组件及所包含的技术服务（安装、调试、现场服务、售后支持等），其单价不高于本次投标价格（即物价指数变动因素后的价格）。

(8) 中标方应承诺：在整个系统运行生命周期内，贵州电网公司有权对平台软件组件应急扩容（扩容的软件组件授权数量不超过本次招标范围的 50%），中标方应配合贵州电网公司进行应急扩容工作。

12.2 质保期要求

“贵州电网公司计量自动化系统 3.0 建设”项目通过竣工验收后开始计算质保期。硬件质保五年；软件授权为永久授权，质保和运维三年，免费提供最新版本升级服务（含大版本升级），并负责安装及运行优化，配合应用开发厂商进行运营部署及优化。本次标包所涉及的病毒库、特征库等具备时效性的数据库，需提供竣工验收后十年的免费离线更新服务。

12.3 技术维护支持

项目通过“贵州电网公司计量自动化系统 3.0 建设”项目整体竣工验收后，进入系统质保期。中标方提供质保期内本标包范围内所有软硬件的技术维护支持，其中，计量自动化系统分布式平台、虚拟化技术平台、智能应用软件、应用性能管理的技术维护应

为原厂维护服务；并协助贵州电网公司与为项目提供设备和软件的第三方达成长期技术维护支持协议。

12.3.1 技术维护支持服务

为保证主站系统开发商及贵州电网公司快速了解本项目供货软件的部署和运维，中标方需要提供相关现场技术支持，直到系统正式上线，业务应用正常使用。技术支持人员随时待命协助贵州电网公司人员维护系统。技术支持服务满足下列要求：

(1) 在“贵州电网公司计量自动化系统 3.0 建设”项目竣工验收后，在质保期内需提供计量自动化系统分布式平台、虚拟化技术平台原厂（提供社保证明）驻场 5x8 小时技术支持服务，驻场人员不少于 6 人。

(2) 投标文件应该包含现场、驻场技术支持人员的有效证件。

(3) 中标方需要提供平台的开发、使用技术规范，指导贵州电网公司建立未来深入业务开发的技术标准和规范。

(4) 对用户如何正常地使用平台进行指导。

(5) 技术支持的范围涵盖系统中所有由中标方提供的以及贵州电网公司委托中标方维护的软硬件。

(6) 紧急技术支持能提供 7x24 小时服务。

(7) 紧急技术支持可采用远程在线诊断的方式。

(8) 可通过电话提供维护。中标方或其他设备供应商指导贵州电网公司人员诊断故障，对于硬件问题，更换发生故障的面板或模块。对平台组件资源开通、日常变更、日常问题等进行处理。

(9) 对平台组件问题进行排查、诊断、定位和修复，和二线工程师对接，直至恢复组件基本功能正常运行。

(10) 若贵州电网公司人员无法解决故障，中标方派维护人员到现场处理。紧急情况下，服务人员要在 4 小时内到达。

(11) 对平台进行日常巡检确保平台稳定运行。

(12) 中标方根据解决问题所需的专门技术，派遣专人处理紧急事件。

(13) 提供设备模块更换服务，更换故障部件。对于发生故障的硬盘，不允许收回故障硬盘，故障硬盘由贵州电网公司自行处理。

(14) 对于紧急递送的请求，用以更换的部件应在 24 小时内送达。

(15) 中标方提供的技术维护服务不得免除中标方所负的质量保证责任。

(16) 了解用户需求，对平台进行优化，提升用户体验。

(17) 熟悉本项目的软件运维，并对贵州电网公司所安排的运维人员进行技术指导。

(18) 驻场技术维护支持人员在近三年负责过 2 个同类型分布式平台运维项目，需提供甲方证明或合同关键页证明（含对应人员名称）。

(19) 具有电力计量采集系统类分布式平台、虚拟化技术平台等运维经验人员优先考虑，需提供证明材料。

(20) 驻场技术支持人员应具备 3 年以上相关工作经验。

12.3.2 备件

(1) 为保证系统可用性，中标方需提供充足的备件。备件应包括：推荐的维修部件和初始提供的运行耗材等。

(2) 所有保修的部/配件需由中标方在 10 天内进行更换，所提供部件必须按原厂型号配置，不得购买除原厂外的第三方部/配件，更换部/配件不得收取费用。

(3) 中标方提供本次所招标建设的系统所需的设备与部件清单，清单包括原厂商的元件编号。中标方提供充足的信息以确保用户可以直接从原厂商处购买设备。该清单应列明所交付的系统各设备和模块的类型和数量。

12.4 二次开发及支持要求

12.4.1 二次开发标准化要求

本项目供货的软件组件（包括但不限于计量自动化系统分布式平台、虚拟化技术平台）应提供完备的贵州电网公司二次开发功能。贵州电网公司可以根据组件提供的二次开发接口，在无须对原来平台的运行程序进行更改情况下，方便的实现二次开发功能。平台提供的贵州电网公司二次开发接口功能及相关资料包括计量自动化系统分布式平台、虚拟化技术平台、智能应用组件、应用性能管理软件等所有列出功能组件的接口，以及未列出但贵州电网公司认为中标方系统中有必要提供的组件的接口。

12.4.2 二次开发的后续支持要求

中标方提供的平台应是一个开放的系统，贵州电网公司或经贵州电网公司同意的任何第三方均可在中标方所提供软件组件（包括但不限于计量自动化系统分布式平台、虚拟化技术平台）的基础上进行新系统集成、新功能开发和第三方的软件集成，中标方应积极的响应和协助配合相关工作，不得以任何理由加以限制或制造障碍。

在工程的实施过程中，需要在平台功能服务的基础上，进一步开展部分功能的开发建设工作，中标方必须提供在系统生命周期内的后续功能建设的技术服务支持。

附件

附件 1：技术建议书编制要求

投标方编制的技术建议书，应包括但不限于如下内容：

1. 技术文件评价索引表

投标方要按照评分要求，总结技术方案优势，编制评分索引表。

2. 技术差异表

投标方要将投标文件和招标文件的差异之处汇集成表。投标单位应如实填写如下“技术差异表”，每项技术条款需说明正偏差、无偏差、负偏差，出现正负偏差的需提供说明材料并建立索引便于查阅。评标专家对是否响应和满足招标文件的全部条款，是否出现非实质性条款负偏差（不满足招标要求）进行审查排序。

技术差异表

序号	项目	技术规范书要求	与技术规范书要求的差异	索引或备注

投标授权代表（签字）

年　　月　　日

3. 总体技术方案

3.1 供货及服务清单

3.1.1. 软件供货清单

针对软件需求清单章节逐一进行回复，提供产品的名称、版本等。

3.1.2. 硬件供货清单

针对硬件需求清单章节逐一进行回复，提供产品的名称、型号、规格等。

3.1.3. 技术服务清单

针对技术服务需求清单章节逐一进行回复，提供技术服务的详细内容。

3.2. 总体技术方案描述

投标方应针对招标技术规范书提出的“一主两域，云边协同”的总体原则，以及技术架构、数据架构、计算架构、云边协同要求、安全架构、典型场景、数据一致性、数据共享、可靠性保障方案、技术创新性等要求，投标方应针对总体技术方案要求，结合投标产品及服务，给出针对本项目的总体技术方案。

4. 关键指标技术响应

重要条款技术指标响应汇总表

序号	产品名称	指标项	技术规范书要求	投标方保证值	响应情况		是否有证明材料	证明材料所在页
					满足	不满足		
1.								
2.								

5. 详细技术方案

投标方应根据招标要求作出详细技术方案：应针对“详细技术方案要求”章节，给出针对本项目的详细技术方案；应针对详细技术方案要求，结合投标产品及服务，对所投软硬件的详细技术进行说明；投标方应报来投标产品规格型号、技术参数、产品使用说明书等资料，如有差异或更好建议配置，需作专门说明。

详细技术方案包括但不限于以下内容：

5.1. 计量自动化系统分布式平台软件解决方案

结合本项目整体建设需求，提供计量自动化系统分布式平台软件解决方案，详细分析并量化计算。

投标方应填写安全 III 区计量自动化系统分布式平台主要软件授权响应情况表。

(1)安全 III 区计量自动化系统分布式平台主要软件授权响应情况表

序号	授权项	授权单位	技术规范书需求的数量	投标数量
1.	运营管理业务可用授权数量	物理机台	317	
2.	运维平台业务可用授权数量	物理机台	317	
3.	云服务器业务可用授权数量	逻辑核	6136	
4.	容器服务业务可用授权数量	逻辑核	6136	
5.	块存储-HDD 业务可用授权数量	TB	141	
6.	对象存储业务可用授权数量	TB	587.52	
7.	事务型关系数据库（TP 库）业务可用授权数量	TB	82.25	
8.	分析型数据库（AP 库）业务可用授权数量	TB	1151.5	
9.	内存数据库业务可用授权数量	GB	3727.5	
10.	企业级分布式应用服务业务可用授权数量	逻辑核	6136	
11.	实时计算业务可用授权数量	逻辑核	2400	
12.	数据离线计算业务可用授权数量	逻辑核	2112	
13.	分布式消息队列业务可用授权数量	TB	58.8	

5.2. 硬件设备解决方案

结合本项目整体建设需求，详细分析并量化计算，提出有针对性的能够实现系统整体运行指标的服务器配置解决方案，以满足系统稳定运行和全链路 1 分钟等性能相关指标的要求。

投标方应填写安全 III 区服务器资源汇总情况表和安全 III 区服务器规模响应情况表、可用容量计算表。

(1)安全 III 区服务器资源汇总情况表

应对本次供货的安全 III 区服务器数量、总 CPU 物理核数、存储容量进行分类汇总，格式如下。

服务器总数（台）	服务器芯片架构	总 CPU 物理核数	总内存容量（TB）	系统盘总容量（TB）	存储总容量		
					SAS SSD（TB）	NVME SSD（TB）	SATA HDD（TB）

(2)安全 III 区设备规模响应情况表

序号	服务器名称	技术规范书需求的数量（台）	投标数量
1.	计量自动化系统分布式平台底座服务器	25	
2.	云服务器	52	
3.	块存储服务器	12	
4.	对象存储服务器	16	
5.	日志服务器	6	
6.	网络服务器	8	
7.	事务型关系数据库服务器	7	
8.	分析型数据库服务器	98	
9.	内存数据库服务器	10	
10.	数据传输服务服务器	3	
11.	实时计算服务器	25	
12.	分布式消息队列服务器	10	
13.	离线计算服务器	22	
14.	数据开发组件服务器	6	
15.	中间件服务器	4	
16.	能力开放组件服务器	3	
17.	安全组件服务器	10	

(3)可用容量计算表

投标方应按照以下表格公式测算所需的可用容量、CPU 等是否满足招标技术要求。

服务器名称	数量	服务器类型	可用容量计算	要求授权量	授权单位
XXX 服务器	XXX	XXX	示例： 3 副本 单台逻辑存储容量=磁盘物理容量[XXX.XXT]*数据磁盘占比[X.00]* 磁盘格式化损耗[0.XX]* 水位线[0.XX]/备份比[X.XXX] = XX.XXT 总的逻辑存储容量=单台服务器存储容量[XX.XXT] * 服务器数量[X] = XXX.XXT	XXXX	TB

5.3. 数据处理解决方案

结合本项目整体建设需求，详细分析并量化，提出有针对性的能够实现系统整体运行指标的数据处理解决方案，项目重点关注的数据处理解决方案如下：

（1）营销系统档案同步一致性及性能要求：以 2348 万用户全量档案为例，投标方详细阐述档案从营销系统同步到系统的内各个数据库或数据湖的解决方案，满足一致性100%的要求，并提供解决方案详细说明及承诺函。

（2）云边协同解决方案，需要详细论证云边协同对应的解决方案，云边协同数据同步性能：以 1 亿条表码数据、1 亿条负荷数据、1 千万条告警数据为例，在南网调度云的云边协同技术框架下，从采集监控域同步到数据分析域。投标方详细阐述在本方所投软硬件配置条件下，最快完成传输的解决方案包括通过数据同步工具、消息队列（API方式）等不同方式下的解决方案，并提供该解决方案承诺函包含各个模式在当前资源条件的同步速率 X 条/秒（格式自拟）。数据分析的配置详见附件中的软硬件配置清单。

（3）分析型数据库具备单集群大规模部署节点的能力，提供解决方案详细说明，如何支撑核心业务的开展。

（4）数据处理（大数据平台）技术方案突出产品成熟度，阐述在能源、政府、金融等重点行业的私有化部署应用情况，提供解决方案详细说明。

（5）投标方认为需要补充的其他内容。

6. 安全技术方案

投标方应针对安全技术方案要求，结合投标产品及服务，给出针对本项目的安全技术方案。

7. 工程进度计划及保障措施

投标方应针对工程进度要求，给出本项目实施部署阶段的具体部署方案，包括但不限于工程进度计划、技术联络会、技术培训计划等。

7.1. 工程进度计划

本项目竣工要求在合同签订之日 14 个月内，或以建设单位通知为准，现场验收（初步验收）要求在合同签订之日 6 个月内，或以建设单位通知为准，投标方案应根据自身

情况详细安排工程的进度。

7.2. 工程进度保障措施

提供详细的保障措施，包括但不限于应急处理方案例如安全要求下更换芯片，产能不足带来的供货能力不足等等；保障工程工期采取相关措施，提前备货等等。

8. 实施方案

投标方应针对项目实施要求和项目验收要求，提供详细的实施方案，应符合计量业务需求，满足海量实时高并发业务场景的数据处理需要。

9. 售后服务承诺

投标方应针对售后服务要求，提供售后服务承诺。

10. 技术研发实力

(1) 技术团队实力

(2) 技术服务能力

11. 其他技术附件

包括但不限于以下内容：

(1) 工程总体兼容性要求承诺书

总体兼容性承诺书

贵州电网有限责任公司：

作为潜在的计量自动化系统分布式平台基础设施的_____投标方，我公司郑重承诺_____公司在计量自动化系统分布式平台基础设施中，承诺所投全部的软硬件产品相互兼容，若出现包括但不限于网络无法互联互通、数据格式不兼容、接口形态不兼容、数据无法互联互通、集成实施后设备运行性能指标低于投标单台设备的性能要求等等各类兼容性问题，由_____公司负责通过调整配置、更换设备、更换配件等等措施，直至解决兼容性问题，费用含在本次投标报价中。

_____公司（盖章）

授权代表（签字）

年　　月　　日

(2) 虚拟化技术平台软件原厂针对硬件设备的兼容性证明

针对服务器、交换机等各一份，格式如下

产品兼容性证明

贵州电网有限责任公司：

作为潜在的计量自动化系统分布式平台基础设施的_____虚拟化技术平台软件产品原厂商，我公司郑重承诺_____公司在计量自动化系统分布式平台基础设施中，所投产品型号：_____的产品与本次项目所投的虚拟化技术平台产品在技术上兼容。

_____公司（盖章）

授权代表（签字）

年　　月　　日

(3) 计量自动化系统分布式平台软件原厂针对硬件设备的兼容性证明

针对服务器、交换机等各一份，格式如下

产品兼容性证明

贵州电网有限责任公司：

作为潜在的计量自动化系统分布式平台基础设施的_____计量自动化系统分布式平台软件产品原厂商，我公司郑重承诺_____公司在计量自动化系统分布式平台基础设施中，所投产品型号：_____的产品与本次项目所投的计量自动化系统分布式平台软件产品在技术上兼容。

_____公司（盖章）

授权代表（签字）

年　　月　　日

(4) 计量自动化系统分布式平台厂商技术路线承诺书

为保障计量自动化系统分布式平台稳定可靠和持续演进，提供所投计量自动化系统分布式平台产品最先进、稳定、安全的版本（截止投标前的版本号及原厂说明书等证明材料），并与该厂商的公有云采用相同架构。提供计量自动化系统分布式平台厂商承诺书（格式如下）

_____（原厂商）

投标计量自动化系统分布式平台软件产品与公有云同架构承诺书

贵州电网有限责任公司：

作为潜在的计量自动化系统分布式平台基础设施的计量自动化系统分布式平台软件产品原厂商，我公司向贵公司郑重承诺如下：

本项目采购的计量自动化系统分布式平台软件产品，我公司向贵公司郑重承诺我公司本次项目投标产品为我司最新版本_____，并且与我司公有云技术路线保持一致，为我公司主流技术架构。

特此承诺。

_____公司（盖章）

授权代表（签字）

年　月　日

(5) 安全自主可控承诺

硬件设备芯片（CPU、GPU 等）、数据库（分布式、集中式）、操作系统（桌面版、服务器版）等核心产品开具安全自主可控承诺书、芯片供应商承诺函、核心芯片应用统计表、核心芯片应用情况表（格式如下）

1．安全自主可控承诺书

贵州电网有限责任公司：

作为潜在的计量自动化系统分布式平台基础设施的产品供应商，我公司向贵公司郑重承诺如下：

本次投标产品：

（1） 硬件设备芯片：（此处替换为投标具体产品名称、型号）

（2） 数据库：（此处替换为投标具体产品名称、版本）

（3） 操作系统：（此处替换为投标具体产品名称、版本）

是_____公司在中华人民共和国境内开发，符合安全可靠测评要求，并承诺在“贵州电网公司计量自动化系统 3.0 建设”项目竣工验收前提供国家权威机构出具的对应产品的证书或认证。

_____公司（盖章）

授权代表（签字）

年　　月　　日

2．芯片供应商承诺函

贵州电网有限责任公司：

我司作为贵公司计量自动化系统分布式平台基础设施服务器(型号：_____）主要核心芯片 [CPU]（型号：_____）的供应商，为保证我司产品的供应稳定，特向贵公司做出如下承诺：

一、关于我方公司注册地及法人的情况

公司名称：

法定代表人姓名：

公司注册地址：

组织机构代码：

我司承诺所提供的公司信息真实有效，公司运营期间公司实际地址将一直保持与注册地址相符。

二、产品信息

芯片设计公司名称：

芯片设计研发地址：

是否拥有该产品的完整齐备设计文件：

芯片制造公司名称：

芯片制造地址（城市）：

芯片封装公司名称：

芯片封装地址（城市）：

芯片测试公司名称：

芯片测试地址（城市）：

我司承诺所提供的产品信息真实有效，并将按贵司要求，如期提供符合质量、数量的产品，采取一切措施，确保供应链的稳定性和连续性，如遇特殊情况可能导致供应中断，将及时通知贵司，并协商采取相应措施，保障产品供应。

特此函达！

供应商：（公章）

3．核心芯片应用统计表

核心芯片应用统计表					
设备类型	设备厂商名称	设备型号	芯片类型	单设备国产芯片数量（颗）	单设备非国产芯片数量（颗）
服务器设备 1			CPU		
			DRAM 颗粒		
			SSD 颗粒		
			网卡芯片		
			电源控制模块芯片		
			BMC		
……			CPU		
			DRAM 颗粒		
			SSD 颗粒		
			网卡芯片		
			电源控制模块芯片		
			BMC		
服务器设备 N			CPU		

			DRAM 颗粒		
			SSD 颗粒		
			网卡芯片		
			电源控制模块芯片		
			BMC		
网络设备 1			CPU		
			DRAM 颗粒		
			FLASH		
			交换/转发芯片		
……			CPU		
			DRAM 颗粒		
			FLASH		
			交换/转发芯片		
网络设备 N			CPU		
			DRAM 颗粒		
			FLASH		
			交换/转发芯片		
安防设备 1			CPU		
			DRAM 颗粒		
			FLASH		
			安全芯片		
……			CPU		
			DRAM 颗粒		
			FLASH		
			安全芯片		
安防设备 N			CPU		
			DRAM 颗粒		
			FLASH		
			安全芯片		

4．核心芯片应用情况表

设备种类	设备型号	芯片种类	芯片描述			芯片设计信息							芯片制造信息		芯片封装信息		芯片测试信息		备注
			芯片厂家	芯片型号	芯片制程（nm）	芯片设计单位	注册地址	注册信息是否包含“集成电路设计”	是否具有独立法人	是否具有集成电路文件核心关键技术和属于本企业的知识产权	是否拥有该集成电路产品的完整齐备设计文件	集成电路设计机构地址（实际研发地点）	芯片制造单位	地址（至少精确到市）	芯片封装单位（全称）	地址（至少精确到市）	芯片测试单位（全称）	地址（至少精确到市）	如果封装测试在一起，就写同样的信息即可
保护类设备（按照招标相关物资品类包含的设备类型填写）	本轮投标供应南方电网设备型号（安全可控）	ADC、CPU、DRAM、FLASH四类	填写填报芯片厂家全名。			填写芯片设计单位全称。													
主站自动化设备	本轮投标供应南方电网设备型号	CPU、SSD、DRAM、BMC、网卡芯片、电源模块控制芯片六类	填写填报芯片厂家全名。			填写芯片设计单位全称。													
安全可控厂站自动化类设备（按照招标相关安全可控物资品类包含的设备类型填写）	本轮投标供应南方电网设备型号	ADC、CPU、DRAM、FLASH、交换/转发芯片五类	填写填报芯片厂家全名。			填写芯片设计单位全称。													

设备种类	设备型号	芯片种类	芯片描述			芯片设计信息							芯片制造信息		芯片封装信息		芯片测试信息		备注
			芯片厂家	芯片型号	芯片制程（nm）	芯片设计单位	注册地址	注册信息是否包含“集成电路设计”	是否具有独立法人	是否具有集成电路文件核心关键技术和属于本企业的知识产权	是否拥有该集成电路产品的完整齐备设计文件	集成电路设计机构地址(实际研发地点)	芯片制造单位	地址（至少精确到市）	芯片封装单位（全称）	地址（至少精确到市）	芯片测试单位（全称）	地址（至少精确到市）	如果封装测试在一起，就写同样的信息即可
厂站自动化类设备（监控主机）	本轮投标供应南方电网设备型号	CPU、SSD、DRAM、BMC、网卡芯片、电源模块控制芯片六类	填写填报芯片厂家全名。			填写芯片设计单位全称。													
安全可控网络安全类设备（安全可控变电站二次安防纵向加密认证装置）	本轮投标供应南方电网设备型号	CPU、DRAM、Flash、安全芯片四类	填写填报芯片厂家全名。			填写芯片设计单位全称。													
安全可控网络安全类设备（安全可控变电站二次安防硬件防火墙）	本轮投标供应南方电网设备型号	CPU、DRAM、FLASH、交换/转发芯片四类	填写填报芯片厂家全名。			填写芯片设计单位全称。													

说明：

1、保护类设备指安全可控 10kV-500kV 保护，其中 10kV-35kV 保护含在安全可控厂站自动化类设备品类，保护类设备具体包括：500kV 线路保护屏（含安全可控和非安全可控）、220kV 线路保护屏（含安全可控和非安全可控）、110kV 线路保护屏（含安全可控和非安全可控）、500kV 母线保护屏（含安全可控和非安全可控）、220kV 母线保护屏（含安全可控和非安全可控）、110kV 母线保护屏（含安全可

控和非安全可控）、500kV 主变保护屏（含安全可控和非安全可控）、220kV 主变保护屏（含安全可控和非安全可控）、110kV 主变保护屏（含安全可控和非安全可控）。

2、安全可控厂站自动化类设备包括照安全可控变电站自动化系统、安全可控智能变电站自动化系统、安全可控变电站时间同步系统、安全可控宽频测量装置及安全可控站控层交换机。

(6) 计量自动化系统分布式平台软件原厂合法授权书

格式如下：

_____（原厂商）

产品销售代理授权书

贵州电网有限责任公司：

作为潜在的计量自动化系统分布式平台基础设施的_____计量自动化系统分布式平台软件产品原厂商，我公司在对销售/集成商的公司规模、技术力量、售后服务、系统集成业绩、商业信誉等方面作出评估之后，推荐_____公司参与上述项目的投标，并郑重授权该公司代理其所投的我公司的产品。

_____公司（盖章）

授权代表（签字）

年　　月　　日

(7) 虚拟化技术平台软件原厂合法授权书

格式如下：

_____（原厂商）

产品销售代理授权书

贵州电网有限责任公司：

作为潜在的计量自动化系统分布式平台基础设施的_____虚拟化技术平台软件产品原厂商，我公司在对销售/集成商的公司规模、技术力量、售后服务、系统集成业绩、商业信誉等方面作出评估之后，推荐_____公司参与上述项目的投标，并郑重授权该公司代理其所投的我公司的产品。

_____公司（盖章）

授权代表（签字）

年　　月　　日

(8) 硬件设备原厂针对本项目出具的合法授权书

服务器、交换机各一份，格式如下

_____（原厂商）

产品销售代理授权书

贵州电网有限责任公司：

作为潜在的计量自动化系统分布式平台基础设施的_____硬件设备生产厂商，我公司在对销售/集成商的公司规模、技术力量、售后服务、系统集成业绩、商业信誉等方面作出评估之后，推荐_____公司参与上述项目的投标，并郑重授权该公司代理其所投的我公司的产品。

_____公司（盖章）

授权代表（签字）

年　　月　　日

(9) 计量自动化系统分布式平台软件原厂技术服务承诺书

内容中包含原厂商的实施服务承诺、售后服务承诺（质保及运维服务自“贵州电网公司计量自动化系统 3.0 建设”项目竣工验收起不少于 3 年）。

格式如下：

_____（原厂商）

技术服务承诺书（云平台软件）

贵州电网有限责任公司：

作为潜在的计量自动化系统分布式平台基础设施的计量自动化系统分布式平台软件产品原厂商，我公司向贵公司郑重承诺如下：

1．负责上述项目中我公司产品在集成商工厂以及用户所在地的安装、部署及调试；

2．对我公司产品提供____年免费运营、运维等技术支持服务，人工、配件、交通等费用全免；

3．对我公司产品提供不少于每天___人时、每周___人天到现场的技术支持；

4．负责我公司产品代理商在投标书中承诺的技术培训。

特此承诺。

_____公司（盖章）

授权代表（签字）

年　　月　　日

(10) 硬件设备原厂针对本项目出具的技术服务承诺书

内容中包含原厂商的实施服务承诺、售后服务承诺（质保及运维服务自“贵州电网公司计量自动化系统 3.0 建设”项目竣工验收起不少于 5 年）。

服务器、交换机各一份，格式如下

_____（原厂商）

技术服务承诺书（硬件设备）

贵州电网有限责任公司：

作为潜在的计量自动化系统分布式平台基础设施的_____硬件设备生产厂商，我公司向贵公司郑重承诺如下：

1．负责上述工程项目中我公司产品在集成商工厂以及用户所在地的安装及调试；

2．对我公司产品提供　　年免费上门维修服务，人工、配件、交通等费用全免；

3．对我公司产品提供不少于___人天到现场的技术支持；

4．负责我公司产品代理商在投标书中承诺的技术培训。

特此承诺。

_____公司（盖章）

授权代表（签字）

年　　月　　日

附件 2 点对点应答文件编制要求

应对本技术规范书的除附件外的全部内容进行点对点应答，单独形成点对点应答文件。点对点应答文件应遵循以下要求编制：

①投标方的《点对点应答文件》中，应说明投标方对本技术规范书的各项要求，描述对各章节的理解程度；

②投标方的《点对点应答文件》中，要求对本技术招标文件所提出的各项要求，各项章节进行逐条逐项答复、说明和解释，首先对实现或满足程度明确做出“满足”、“部分满足”、“不满足”等应答。如投标方对某些部分不能满足、部分满足本招标文件要求时,需详细说明原因,明确满足招标文件要求的时限，并承诺今后免费提供该设备或服务；

③凡在《点对点应答文件》中答复为“满足”的，双方均视其为无条件满足。若有附加条件的，双方均视其为“部分满足”。如答复为规定格式之外其它内容的，均视为“不满足”；

④投标方在对本招标文件作完整答复的前提下，应将答复为“部分满足”、“不满足”的有关条款及其解释单独列出，汇编为正式文档提交给贵州电网公司；

⑤凡《点对点应答文件》的答复与其《技术方案》的其他部分或报价书有出入的，以《点对点应答文件》的答复为准，由此产生的一切后果，由投标方负责。

附件 3 政府采购需求标准

本项目涉及的服务器、数据库、操作系统以及运维终端等软硬件设备，还应当满足以下政府采购需求标准当中加“*”的指标参数要求。

1. 通用服务器采购需求标准

序号	指标分类	一级指标	二级指标	指标要求
1.	产品规格	*CPU 规格	*CPU 信息	供应商给出 CPU 信息，包含 CPU 型号、物理核心数、主频、末级缓存容量、线程数、热设计功耗及支持内存的最高速率、通道数和位宽
2.	产品规格	*主板规格	*主板支持的 CPU 和内存情况	供应商给出主板支持的 CPU 和内存的型号数量
3.	产品规格		*主板内存槽数量	非板载内存的可扩展插槽数量应不少于 4 个
4.	产品规格		*主板存储接口	至少支持 SATA、SAS、M.2、U.2 等存储接口中的 1 种
5.	产品规格		*PCIe 插槽接口	符合 PCIe3.0 或以上的高速串行计算机扩展总线标准，PCIe 的接口速率与位宽需保证向下兼容
6.	产品规格		*主板 PCIe 插槽数量及规格	(1)高度大于 44.45mm 双路或以上服务器 PCIe 插槽或接口应不少于 5 个； (2)单路服务器 PCIe 插槽或接口应不少于 4 个，可通过扩展卡进行插槽扩展
7.	产品规格	*内存规格	*内存数量	≥4
8.	产品规格		*内存规格	≥DDR4
9.	产品规格		*内存通道	支持多个内存接口通道，每个通道可支持 1DPC 或 2DPC，当支持 2DPC 时，印制电路板上应具备插槽的序号标识，具体通道数应在随机文件中明确
10.	产品规格	*存储规格	*硬磁盘实配容量	服务器产品至少要配备一款存储设备 (1)若配备硬磁盘，服务器提供的实配硬磁盘可用容量应不小于 600GB (2)若配备固态盘，实配固态盘单盘可用容量不小于 480GB，NVMe SSD 容量不小于 960GB
11.	产品规格		*硬盘实配数量	(1)若配备硬磁盘，服务器提供的实配硬磁盘数量应不小于 2 块，可实现互为备份； (2)若配备固态盘，实配盘数应不小于 1 块
12.	产品		*硬盘插槽数	(1)供应商应给出配置的硬盘尺寸，如 2.5 英

序号	指标分类	一级指标	二级指标	指标要求
	规格		量及规格	寸、3.5 英寸硬磁盘； (2)机箱高度为 88.9mm 的服务器可支持的硬盘数量应不少于 8 块，机箱高度为 44.45mm 的服务器可支持的硬盘数量应不少于 4 块。 (3)存储型服务器可支持硬盘数量应不少于 24 块
13.	产品规格	*网络规格	*网口速率和数量	配备网口数量不少于 1 个，且网口速率不少于 1GE
14.	产品规格	*外部接口规格	*显示接口	显示接口类型应不少于 1 种，如：VGA、DP、HDMI 等
15.	产品规格		*USB 接口	配备 USB 接口，如 USB2.0、USB3.0 等
16.	产品规格	*电源规格	*电源模块数量	≥2
17.	产品规格		*电源功率	电源模块功率应有一定冗余，满足处理器满载时的需求
18.	产品规格	*整机规格	*外观和结构	(1)服务器的零部件应紧固无松动，可插拔部件应可靠连接，开关、按钮和其它控制部件应灵活可靠，布局应方便使用； (2)产品表面不应有明显的凹痕、划伤、裂缝、变形和污染等。表面涂层均匀，不应起泡、龟裂、脱落和磨损，金属零部件无锈蚀及其它机械损伤； (3)产品表面说明功能的文字、符号和标志应清晰、端正且牢固； (4)应在服务器的显著位置提供运行状态的指示功能，并在随机文件中明确具体含义； (5)机架、机箱的尺寸应符合通用机柜的安装要求，插入总线插座的电路板接口外形尺寸应符合有关总线标准的规定，将机箱固定在机柜上，机箱底面最大下垂变形不得干涉相邻机体； (6)高密度服务器应给出 CPU 个数与机柜高度； (7)服务器尺寸具体要求在随机文件中明确
19.	产品规格		*尺寸（高×宽×深）	供应商给出产品尺寸；设计应遵循标准化、系列化的要求；机箱的内部结构符合通用部件的安装需要
20.	产品规格		*环境适应性	气候环境适应性应符合 GB/T9813.3 的有关规定，工作温度 10~35℃，贮存运输温度-40～55℃；工作相对湿度 35%～80%，贮存运输相对湿度 20％～93%（40℃)；大气压 86～106kPa
21.	产品		*机械环境适	机械环境适应性应符合 GB/T9813.3 的有关规

序号	指标分类	一级指标	二级指标	指标要求
	规格		应性	定
22.	产品规格		*噪声	符合 GB/T 9813.3 的有关规定，在产品说明中给出具体测试值 塔式服务器噪声在空闲状态下不大于 50dB
23.	产品规格	机柜规格	*机柜尺寸	供应商给出长度、高度和深度
24.	功能要求	*主板功能	*主板外部接口种类	支持 USB、显示、管理等接口，如： VGA、DP、HDMI、USB3.0、PS/2 接口、BMC 管理端口
25.	功能要求	*网络功能	*网络功能	支持网络连接、网络访问、数据交换和网络管控功能
26.	功能要求	*CPU 功能	*计算处理	支持通用计算及虚拟化功能。处理器需集成整型计算单元、浮点计算单元、内存控制器、I/O 模块等，处理器与存储部件、网络部件、I/O 部件等组成计算系统，提供数据处理、网络接入等计算相关功能
27.	功能要求		*密码算法实现	CPU 芯片应符合 GM/T 0008 的相关规定，或芯片密码模块应符合 GB/T37092 或 GM/T 0028 的相关规定
28.	功能要求	*电源功能	*电源热插拔	整机电源模块应具备热插拔功能
29.	功能要求		*电源过流保护	支持过流及短路保护的功能
30.	功能要求	*整机功能	*散热方式	支持风冷等散热方式
31.	功能要求	*管理系统功能	*BMC 固件基础功能	(1)支持 DHCP 设置网络功能； (2)支持静态 IP 设置网络功能； (3)支持设备日志记录，包括但不限于登录日志、操作日志和报警日志等功能； (4)支持日志信息导出和记录删除功能； (5)支持通过管理接口向外输出准确的报警信息功能； (6)设备的 BMC 管理软件应能够按报警的严重程度进行区分； (7)支持 IPMI2.0、SNMP 或 Redfish 等接口功能； (8)支持键盘、鼠标和视频的重定向、文本控制台的重定向、远程虚拟媒体、高可靠的硬件监控和管理功能； (9)支持基于网络开启、关闭和重启设备的功能，并查询当前设备开机运行状态； (10)支持故障提示功能，并可通过接口读取服务器故障信息；

序号	指标分类	一级指标	二级指标	指标要求
				(11)支持基于网络的固件更新功能，包括 BMC 和 BIOS 等； (12)支持基于网络安装操作系统的功能，并可通过网络控制台访问设备； (13)支持通过本地的硬盘或光驱等存储设备，基于网络完成设备的操作系统安装功能； (14)支持通过浏览器打开管理界面并登录功能； (15)支持设置口令策略功能； (16)支持访问权限设置功能，并通过日志记录访问事件； (17)支持对出厂默认的用户名及口令进行安全保护功能，并提供默认口令修改提示； (18)支持读取设备主板的工作环境温度功能； (19)支持读取服务器 CPU 等核心器件的温度功能； (20)支持通过外部管理工具进行 BMC 参数设置的功能，并可基于网络通过外部管理工具对 BMC 进行管理； (21)应支持固件版本查询、固件升级 (22)支持基于网络实现开关机和复位控制的功能； (23)BMC 启动时间应不超过 180s，实现功能包括网络、IPMI、散热、传感器服务可用； (24)支持 BMC 固件设置的恢复出厂功能
32.	功能要求		*BIOS 固件基础功能	(1)支持查看固件版本、内存信息、主板信息、处理器信息和系统时间信息功能； (2)支持上电初始化界面显示 CPU 信息、内存信息、固件版本和部分快捷键信息功能； (3)支持设置界面中英文显示切换功能； (4)支持查看 PCIe 设备信息，SATA 设备信息功能； (5)支持操作系统安装和引导功能，应并向操作系统提供计算机主板信息和服务接口； (6)支持设置启动顺序，并按照设置的启动顺序启动功能； (7)支持安全启动功能； (8)支持设置口令、修改口令、验证口令功能； (9)支持板载显示控制或独立显卡的显示控制功能； (10)支持 RAID 识别和启动功能； (11)支持串口重定向功能； (12)支持固件更新功能；

序号	指标分类	一级指标	二级指标	指标要求
				(13)支持 BIOS 固件设置的恢复出厂功能； (14)支持网络引导启用和关闭功能
33.	功能要求		*远程控制	支持远程关机和重新启动功能
34.	功能要求	*操作系统及驱动功能	*操作系统及驱动的升级	支持通过网络、闪存盘对操作系统、驱动进行升级
35.	功能要求		*操作系统功能	(1)支持访问控制、安全审计、网络接入鉴别等功能； (2)操作系统其他功能应满足操作系统政府采购需求标准中加*的指标要求
36.	功能要求	*中文信息处理功能	*中文信息处理	符合 GB 18030 的有关规定
37.	安全要求	*关键部件安全要求	*关键部件安全要求	CPU 和操作系统等关键部件应当符合安全可靠测评要求
38.	安全要求	*固件安全要求	*故障检测	支持故障检测功能，可以检测到具体的 FRU（内存、硬盘等）的故障并发出告警
39.	安全要求	*系统安全要求	*弱口令字典检查	支持弱口令字典检查功能，出现在弱口令字典中的字符串不能被设置为用户口令
40.	安全要求		*白名单访问控制	支持基于时间、IP 或 MAC 白名单访问控制
41.	安全要求		*二次鉴别	支持二次鉴别功能。对于用户配置、权限配置、公钥导入等重要的管理操作，已登录用户应通过二次鉴别后，才能执行操作
42.	安全要求		*密码证书安全加密存储	支持对带外管理系统中的用户口令和证书等敏感信息进行加密存储，禁止使用私有的和业界已知不安全的密码算法
43.	安全要求		*敏感信息安全加密传输	支持使用安全的传输加密协议（如 SSH 或 HTTPS 等）传输用户的敏感信息
44.	安全要求	*信息安全要求	*研发过程安全	供应商承诺，生产商已建立从需求、设计、开发、测试、维护端到端的开发流程管理机制，输出和保存开发流程中每个阶段的产品需求清单、设计文档、开发文档、测试记录等材料，保证各个流程可追溯
45.	安全要求	*物理安全	*物理安全	安全要求应符合 GB 4943.1 的规定
46.	安全要求	*限用物质的限量要求	*限用物质的限量要求	限用物质的限量应符合 GB/T 26572 的要求
47.	性能要求	*CPU 性能	*CPU 主频	≥1.8GHz
48.	性能要求		*单 CPU 核数	≥4
49.	性能要求		*单 CPU 末级缓存容量	≥8MB

序号	指标分类	一级指标	二级指标	指标要求
50.	性能要求	*内存性能	*内存速率	≥2666MT/s
51.	性能要求	*电源能耗	*电源能耗	符合 GB/T 9813.3 的有关规定
52.	兼容要求	*部件兼容性要求	*内存兼容性	适配 3 种及以上厂商的内存产品，且均不低于产品支持的内存规格
53.	兼容要求		*固态存储兼容性	适配 3 种或以上厂商的固态存储产品，且均不低于产品支持的固态存储设备规格
54.	兼容要求		*网卡兼容性	网卡应适配两种或以上厂商产品
55.	兼容要求		*功能卡兼容性	内置或适配符合 PCIe 的功能卡，如：网络功能卡、存储功能卡及图形显示功能卡
56.	兼容要求	*外设兼容性	*外设兼容性	兼容多种主流生产商的外部设备，包括显示器、键盘、鼠标、闪存盘、移动硬盘、USB 光驱及 KVM 等，要求使用不同厂商的外部设备时，系统均能正常识别和安装驱动
57.	兼容要求	*软件兼容性	*数据库兼容	兼容 3 个及以上厂商的数据库产品
58.	兼容要求		*中间件兼容	兼容 3 个及以上厂商的中间件产品
59.	兼容要求		*平台软件兼容	兼容 3 个及以上厂商的大数据平台
60.	可靠性要求	*整机可靠性要求	*整机可靠性	m1 值（MTBF 的不可接受值）不得低于 30000h
61.	可靠性要求		*风扇可靠性	风扇寿命应不低于 40000h
62.	可靠性要求		*部件可靠性	支持硬盘、电源、风扇热插拔(内置风扇除外)
63.	包装及运输要求	*包装及运输要求	*标志、包装、运输和贮存	符合 GB/T 9813.3 和商品包装政府采购需求标准的相关规定
64.	服务要求	*服务响应	*服务响应	(1)提供电话、电子邮件、远程连接等多种形式服务； (2)提供同城 4h、异地 12h 技术响应服务，2 个工作日解决问题，对于未能解决的问题和故障应提供可行的升级方案，并提供周转设备； (3)建立全国技术服务体系和服务团体，符合专业服务体系标准要求，提供原厂中文服务；

序号	指标分类	一级指标	二级指标	指标要求
				(4)服务周期内提供产品的维修、换件和升级服务
65.	服务要求		*培训服务	供应商提供培训材料、产品手册、培训视频等培训相关内容
66.	服务要求	*服务周期	*服务周期	(1)产品免费服务周期（含换件和维修）应不小于 3 年； (2)设备停产后继续提供质量保障服务（含备品备件），服务终止时间与最后一批设备交付时间间隔不低于 6 年； (3)产品停止服务时间应提前 1 年告知客户； (4)产品发布日期需在随机文件中明确
67.	服务要求	*服务工具要求	*工具要求	供应商提供设置服务器硬件、辅助操作系统安装等功能的辅助工具和管理软件。且随附软件应具有合法授权或版权
68.	服务要求		*驱动安装升级指引	供应商提供出厂安装的配件所需的驱动程序，形式包括但不限于驱动光盘、驱动下载链接等。其他配件应提供指引
69.	服务要求		*管理软件	具备资源管理、系统管理、性能监控、健康监控、基于网络控制、报警设置功能
70.	服务要求	*增值服务	*厂家升级产品软件与扩容服务	供应商提供原厂级的部件/软件产品升级和扩容能力
71.	服务要求		*提供上门服务	供应商具备提供上门服务的能力
72.	供保要求	*供应链质量	*抗干扰性	当产品部件出现供应风险时，应通知客户并提供风险应对方案确保产品的服务保障，必要时应停止相关受影响产品的销售
73.	供保要求		*供应能力证明	供应商提供供应链稳定承诺书，确保产品的部件在产品服务周期内稳定供货

2. 数据库采购需求标准

2.1. 分布式数据库

序号	指标分类	一级指标	二级指标	指标要求
1.	功能要求	*安装与升级	*数据库安装	(1)支持命令行或图形化的安装； (2)支持命令行或图形化的可配置安装能力； (3)依据安装环境提供相应的初始化参数配置值； (4)提供图形化软件组件管理向导工具
2.	功能要求		*数据库重启	(1)支持命令行或图形化的方式关闭和启动服务；

序号	指标分类	一级指标	二级指标	指标要求
				(2)关闭服务后，再启动服务，服务正常
3.	功能要求		*安装配置日志	(1)提供软件安装的日志记录功能； (2)记录的软件安装信息完整正确； (3)提供安装配置操作的日志记录功能； (4)记录的配置操作信息完整正确
4.	功能要求		*升级维护	(1)支持版本升级，保证版本间功能和数据的兼容性； (2)厂商提供当前版本与历史版本的差异说明文档，包含新版本对软件和硬件的支持情况
5.	功能要求	*数据配置	*参数配置	(1)依据工作负载和运行环境，提供配置参数修改的能力； (2)修改数据库配置参数后，配置参数立即生效或数据库重新启动生效，立即生效的配置参数和需要数据库重新启动方可生效的配置参数应在相关文档中明确
6.	功能要求	*SQL 功能	*基础数据类型	(1)支持数值类型； (2)支持字符类型； (3)支持二进制类型； (4)支持日期和时间类型； (5)支持布尔类型； (6)支持（大）文本类型； (7)支持大对象类型
7.	功能要求		*数据存储基础功能	支持基础数据类型
8.	功能要求		*数据检索基础功能	支持基础数据类型
9.	功能要求		*核心 SQL 能力	(1)支持左外连接； (2)支持右外连接； (3)支持内连接； (4)支持全连接
10.	功能要求		*字符集	中文字符集符合 GB 18030 的要求
11.	功能要求		*常用操作符	(1)支持逻辑操作符及相关运算； (2)支持比较操作符及相关运算； (3)支持算术运算符及相关运算
12.	功能要求		*条件表达式	(1)支持对比条件表达式； (2)支持逻辑条件表达式； (3)支持空值条件表达式； (4)支持等于条件表达式； (5)支持模式匹配条件表达式； (6)支持区间条件表达式； (7)支持 IN 条件表达式； (8)支持存在条件表达式；

序号	指标分类	一级指标	二级指标	指标要求
				(9)支持以上条件表达式的复合表达式
13.	功能要求		*SQL 执行计划	支持 SQL 计划，使 SQL 按照指定的语句执行，并实现预期结果
14.	功能要求	*数据库对象	*基础对象类型	(1)支持用户的创建、删除、修改； (2)支持角色的创建、删除、修改； (3)支持存储过程的创建、删除、修改； (4)支持表操作功能； (5)支持自增序列； (6)支持主键约束、唯一性约束、检查约束和联合主键约束； (7)支持游标功能； (8)支持视图的创建、删除、修改； (9)支持数值计算函数、字符处理函数、日期时间值函数、间隔函数、类型转换函数、位运算函数、聚合函数、格式化、系统信息等常用函数
15.	功能要求		*基础表分区管理	(1)哈希分区方式； (2)范围分区方式； (3)列表分区方式
16.	功能要求		*对象变更	(1)支持数据库的创建、删除、更新以及数据库属性的查询； (2)支持在线变更表结构、索引； (3)支持数据的增加、删除、修改和查询
17.	功能要求	*事务能力	*事务基础特性	支持事务的 ACID
18.	功能要求		*死锁检测与处理	(1)在并发执行过程中，能检测到死锁； (2)提供解决全局死锁的机制； (3)具备死锁处理能力； (4)具备死锁超时回滚的能力； (5)具备死锁检测与处理记录功能
19.	功能要求	*运维	*运行时统计信息基础功能	(1)数据库慢 SQL 统计： 1．支持统计 SQL 语句； 2．支持统计用户名； 3．支持统计数据库名； 4．支持统计执行时长； (2)数据库性能状态统计： 1．支持统计每秒事务数和查询数； 2．支持统计 SQL 平均响应时间； 3．支持统计高频 SQL
20.	功能要求		*日志	(1)具备对各类事件进行日志记录的功能，可通过日志查看操作内容、执行过程和结果； (2)具备提示和警告功能，提示或警告数据库结构修改、数据库运行配置修改等重要操作；

序号	指标分类	一级指标	二级指标	指标要求
				(3)日志完整正确，并且提供可读文本的形式； (4)支持中文日志
21.	功能要求		*远程运维	具备远程维护功能
22.	功能要求		*报警	(1)厂商提供通知管理员的方法或工具； (2)支持设置报警基线，数据库运行中遇到重要事件、异常事件和状态、超过报警阈值等情况时，通知管理员； (3)提供报警 API； (4)报警发生时，支持报警信息的实时展示
23.	功能要求	*迁移	*数据迁移	(1)提供元数据、数据库、数据库对象、表数据快速迁移的功能； (2)支持数据迁移工具实现同构或异构数据库之间的数据迁移； (3)支持全量数据迁移、增量数据持续同步等迁移模式； (4)在数据迁移过程中具备应对传输异常的能力，保障数据迁移的稳定性、连续性和一致性； (5)支持存量数据的一次性迁移和增量数据库的持续同步； (6)支持多种不同类型的源数据库和目标数据库之间的数据迁移
24.	功能要求		*数据比对基础功能	对源数据库和目标数据库之间的数据进行比对，支持数据一致性，并提供一致性比对报告
25.	功能要求	*备份恢复	*数据备份	(1)运行状态下支持对数据库进行全库备份； (2)运行状态下支持对数据库进行部分备份； (3)运行状态下支持对数据库进行增量备份
26.	功能要求		*多种存储媒体备份、还原	支持多种备份存储媒体，支持多种存储媒体的部分、完整数据库数据还原处理能力
27.	功能要求		*备份还原的一致性校验	提供数据库备份数据一致性校验的命令或工具
28.	功能要求	*集群管理	*集群构建与管理	(1)支持集群的运行环境； (2)支持创建并配置数据库集群； (3)配置信息至少包括日常运维管理、容灾管理、日志管理、备份管理、监控等
29.	功能要求		*数据分布	(1)支持自动数据分布； (2)按照指定规则设置数据分布
30.	功能要求		*分布式计算	支持在分布式节点上的并行计算
31.	功能要求		*集群扩展	(1)支持在线扩容、缩容； (2)集群扩容、缩容过程中支持分布式事务 ACID 特性
32.	功能		*数据重分布	支持按照数据库集群的节点、状态和负载的变

序号	指标分类	一级指标	二级指标	指标要求
	要求			化，进行动态重分布
33.	功能要求		*对应用透明	当数据分布、分布计算、集群扩展、数据重分布等变化时，不需要修改应用代码
34.	功能要求		*均分负载	支持在集群环境下，事务并行执行
35.	功能要求	*工具	*数据库开发调试工具	(1)具备图形化功能，提高易用性； (2)具备导入、编辑、保存、执行 SQL 语句和 SQL 脚本功能； (3)具备复制、编辑现有数据库对象功能； (4)具备关键词显示标记、动态语法提示的 SQL 编辑器功能
36.	功能要求		*用户、角色管理工具	(1)支持创建、修改、删除用户的功能； (2)提供定义用户的功能； (3)支持创建、修改、删除角色的功能，且提供用户自定义角色的功能
37.	功能要求		*SQL 执行计划查看工具	(1)提供与数据库管理系统进行 SQL 交互的工具，方便运维工作； (2)支持查看 SQL 语句查询执行计划与统计信息
38.	功能要求		*数据库对象工具	(1)支持创建、修改、删除表的功能，支持定义表结构、约束、存储配置管理的功能； (2)支持创建、修改、删除索引的功能，支持定义索引结构、类型、存储配置管理的功能； (3)支持创建、修改、删除视图的功能，支持视图定义的功能； (4)支持创建、修改、删除约束的功能，支持约束定义的功能
39.	功能要求		*导入导出工具	(1)支持导出不同格式，可以将不同格式数据导入到数据库中； (2)支持不同级别和不同数据库对象的导入/导出功能； (3)支持从文本文件或者其他上游数据源将数据导入； (4)支持 SQL 脚本进行导入导出
40.	功能要求		*数据库运维工具	(1)支持数据库、数据库存储对象结构、数据、统计信息更新维护； (2)支持数据库创建、数据库修改、数据库删除、数据库模板维护； (3)支持数据库任务自动化调度作业管理； (4)支持图形化展示数据库管理的各种元数据界面，展示的内容具有层次性，包括模式、非模式数据字典信息
41.	功能	*图形化管	*图形化的开	厂商提供图形化的开发工具

序号	指标分类	一级指标	二级指标	指标要求
	要求	理	发工具	
42.	功能要求		*图形化运维工具	厂商提供图形化的运维工具
43.	可靠性要求	*稳定运行	*稳定运行	(1)支持连续稳定运行； (2)支持数据库管理系统运行风险的报警能力
44.	可靠性要求	*故障切换	*快速切换	支持快速切换，在主数据库出现故障时，能够快速切换到备用数据库，保障业务正常运行
45.	可靠性要求		*恢复无断点	支持无断点恢复能力
46.	可靠性要求	*容灾能力	*主备备份	(1)支持多副本，支持主副本与从副本之间的数据同步，最低时延由生产厂商提供； (2)提供数据库复制技术，包括基于日志的备用数据库远程数据库备份技术，并具备数据副本间的复制能力
47.	可靠性要求		*实例容灾	(1)在任意数据库实例出现故障时，集群内服务正常运行，数据不丢失，集群整体业务可用； (2)在实例故障、节点故障等单数据库实例故障时，RPO 时间等于 0，RTO 时间小于 30s
48.	可靠性要求		*容灾部署	(1)提供远程容灾部署与管理功能； (2)提供生产中心与备份中心之间的容灾部署与管理功能
49.	可靠性要求		*同城容灾	(1)支持同城双中心部署，当主中心故障时，业务切换到备中心； (2)由于网络、供电等原因造成的可用区级故障，触发集群计划外停机，在同城多可用区场景下，RPO 时间等于 0，RTO 时间小于 1 分钟
50.	可靠性要求	*容错性	*服务端编程稳定性	支持当用户自定义的存储过程、函数运行异常时，数据库稳定运行
51.	可靠性要求		*网络容错	网络中断时，保障事务一致性
52.	可靠性要求		*检测报警	(1)支持数据库实例启动时错误检测能力； (2)支持加载不同文件格式、不同大小数据出现错误时的故障检测和处理能力； (3)支持数据库备份执行过程中发生故障时报错或者报警能力； (4)支持数据库恢复发生故障时报错或者报警能力

序号	指标分类	一级指标	二级指标	指标要求
53.	可靠性要求		*故障恢复	(1)系统故障重启后能正常运行且支持数据一致性； (2)支持完全媒体故障恢复的能力； (3)提供基于时间点故障恢复功能
54.	可靠性要求		*不同级别故障可恢复	支持数据库事务故障、系统故障、存储媒体故障不同级别的可恢复能力
55.	兼容要求	*软件兼容	*云化部署	支持虚拟化部署或容器化部署等云化部署方式
56.	兼容要求	*硬件兼容	*硬件平台兼容	(1)同源支持以下至少三种 CPU 平台架构： 1.ARM； 2.LoongArch； 3.MIPS； 4.SW64； 5.x86； (2)支持 SMP 和 NUMA 的运行环境
57.	兼容要求	*标准兼容	*ODBC	支持 ODBC
58.	兼容		*JDBC	支持 JDBC
59.	服务要求	*交付方式	*交付方式	以光盘、便携式移动设备、镜像文件、在线下载等交付方式提供产品交付物
60.	服务要求	*服务周期	*产品维护周期	产品自发布之日起至产品停止功能升级（包含不限于新特性、新硬件支持、问题修复、安全补丁等）之日止≥5 年
61.	服务要求		*产品延伸服务周期	产品停止功能升级之日起至产品停止功能维护（包括问题修复、安全补丁等）之日止≥4 年
62.	服务要求		*产品延伸安全服务周期	产品功能维护停止之日起至产品停止安全维护（包括中高风险漏洞修复）之日止≥2 年
63.	服务要求		*售后服务最小保障期	自销售之日起，产品售后服务周期≥6 年
64.	服务要求	*供应链与服务保障	*供应链与服务保障基础要求	(1)提供多种形式支持服务，包含电话、电子邮件、远程连接等； (2)提供技术支持服务，支持同城 4h、异地 12h 响应要求，两个工作日解决问题，对于未能解决的问题和故障提供可行的升级方案； (3)提供培训材料、产品手册、培训视频等培训相关内容； (4)建立全国技术服务体系和服务团队，符合专业服务体系标准要求，提供原厂中文服务； (5)服务周期内支持版本免费升级； (6)开源产品对获得的社区源代码进行安全性和知识产权审查与管理；

序号	指标分类	一级指标	二级指标	指标要求
				(7)提供数据库参数、慢 SQL 语句的性能优化指南，包含性能优化的具体措施、技巧、案例及建议等；
65.	安全要求	*基本要求	*基本要求	数据库应当符合安全可靠测评要求
66.	安全要求	*基础安全	*漏洞管理	建立漏洞管理机制，及时通过邮件、网站等方式将安全漏洞告知用户，并提供安全补丁对漏洞进行修复
67.	安全要求		*身份鉴别及访问控制	提供身份鉴别及访问控制，加解密的密码要求符合 GM/T0028 的相关规定

2.2.集中式数据库

序号	指标分类	一级指标	二级指标	指标要求
1.	功能要求	*安装与升级	*数据库安装	(1)支持命令行或图形化的安装； (2)支持命令行或图形化的可配置安装能力； (3)依据安装环境提供相应的初始化参数配置值； (4)提供图形化软件组件管理向导工具
2.	功能要求		*数据库重启	(1)支持命令行或图形化的方式关闭和启动服务； (2)关闭服务后，再启动服务，服务正常
3.	功能要求		*安装配置日志	(1)提供软件安装的日志记录功能； (2)记录的软件安装信息完整正确； (3)提供安装配置操作的日志记录功能； (4)记录的配置操作信息完整正确
4.	功能要求		*升级维护	(1)支持版本升级，保证版本间功能和数据的兼容性； (2)厂商提供当前版本与历史版本的差异说明文档，包含新版本对软件和硬件的支持情况
5.	功能要求	*数据配置	*参数配置	(1)依据工作负载和运行环境，提供配置参数修改的能力 (2)修改数据库配置参数后，配置参数立即生效或数据库重新启动生效，立即生效的配置参数和需要数据库重新启动方可生效的配置参数在相关文档中明确
6.	功能要求	*SQL 功能	*基础数据类型	(1)支持数值类型； (2)支持字符类型； (3)支持二进制类型； (4)支持日期和时间类型； (5)支持布尔类型； (6)支持（大）文本类型；

序号	指标分类	一级指标	二级指标	指标要求
				(7)支持大对象类型
7.	功能要求		*数据存储基础功能	支持基础数据类型
8.	功能要求		*数据检索基础功能	支持基础数据类型
9.	功能要求		*核心 SQL 能力	(1)支持左外连接； (2)支持右外连接； (3)支持内连接； (4)支持全连接
10.	功能要求		*字符集	中文字符集符合 GB 18030 的要求
11.	功能要求		*常用操作符	(1)支持逻辑操作符及相关运算； (2)支持比较操作符及相关运算； (3)支持算术运算符及相关运算
12.	功能要求		*条件表达式	(1)支持对比条件表达式； (2)支持逻辑条件表达式； (3)支持空值条件表达式； (4)支持等于条件表达式； (5)支持模式匹配条件表达式； (6)支持区间条件表达式； (7)支持 IN 条件表达式； (8)支持存在条件表达式； (9)支持以上条件表达式的复合表达式
13.	功能要求		*SQL 执行计划	支持 SQL 计划，使 SQL 按照指定的语句执行，并实现预期结果
14.	功能要求	*数据库对象	*基础对象类型	(1)支持用户的创建、删除、修改； (2)支持角色的创建、删除、修改； (3)支持存储过程的创建、删除、修改； (4)支持表操作功能； (5)支持自增序列； (6)支持主键约束、外键约束、唯一性约束、检查约束和联合主键约束； (7)支持游标功能； (8)支持视图的创建、删除、修改； (9)支持数值计算函数、字符处理函数、日期时间值函数、间隔函数、类型转换函数、位运算函数、聚合函数、格式化、系统信息等常用函数
15.	功能要求		*基础表分区管理	(1)哈希分区方式； (2)范围分区方式； (3)列表分区方式
16.	功能要求		*对象变更	(1)支持数据库的创建、删除、更新以及数据库属性的查询；

序号	指标分类	一级指标	二级指标	指标要求
				(2)支持在线变更表结构、索引； (3)支持数据的增加、删除、修改和查询
17.	功能要求	*事务能力	*事务基础特性	支持事务的 ACID
18.	功能要求		*死锁检测与处理	(1)在并发执行过程中，能检测到死锁； (2)提供解决全局死锁的机制； (3)具备死锁处理能力； (4)具备死锁超时回滚的能力； (5)具备死锁检测与处理记录功能
19.	功能要求	*运维	*运行时统计信息基础功能	(1)数据库慢 SQL 统计： 1.支持统计 SQL 语句； 2.支持统计用户名； 3.支持统计数据库名； 4.支持统计执行时长； (2)数据库性能状态统计： 1.支持统计每秒事务数和查询数； 2.支持统计 SQL 平均响应时间； 3.支持统计高频 SQL
20.	功能要求	*运维	*日志	(1)具备对各类事件进行日志记录的功能，可通过日志查看操作内容、执行过程和结果； (2)具备提示和警告功能，提示或警告数据库结构修改、数据库运行配置修改等重要操作； (3)日志完整正确，并且提供可读文本的形式； (4)支持中文日志
21.	功能要求		*远程运维	具备远程维护功能
22.	功能要求		*报警	(1)厂商提供通知管理员的方法或工具； (2)支持设置报警基线，数据库运行中遇到重要事件、异常事件和状态、超过报警阈值等情况时，通知管理员； (3)提供报警 API； (4)报警发生时，支持报警信息的实时展示
23.	功能要求	*迁移	*数据迁移	(1)提供元数据、数据库、数据库对象、表数据快速迁移的功能； (2)支持数据迁移工具实现同构或异构数据库之间的数据迁移； (3)支持全量数据迁移、增量数据持续同步等迁移模式； (4)在数据迁移过程中具备应对传输异常的能力，保障数据迁移的稳定性、连续性和一致性； (5)支持存量数据的一次性迁移和增量数据库的持续同步； (6)支持多种不同类型的源数据库和目标数据

序号	指标分类	一级指标	二级指标	指标要求
				库之间的数据迁移
24.	功能要求		*数据比对基础功能	对源数据库和目标数据库之间的数据进行比对，支持数据一致性，并提供一致性比对报告
25.	功能要求	*备份恢复	*数据备份	(1)运行状态下支持对数据库进行全库备份； (2)运行状态下支持对数据库进行部分备份； (3)运行状态下支持对数据库进行增量备份
26.	功能要求		*多种存储媒体备份、还原	支持多种备份存储媒体，支持多种存储媒体的部分、完整数据库数据还原处理能力
27.	功能要求		*备份还原的一致性校验	提供数据库备份数据一致性校验的命令或工具
28.	功能要求	*集群管理	*集群构建与管理	(1)支持集群的运行环境； (2)支持创建并配置数据库集群； (3)配置信息至少包括日常运维管理、容灾管理、日志管理、备份管理、监控等
29.	功能要求	*工具	*数据库开发调试工具	(1)具备图形化功能，提高易用性； (2)具备导入、编辑、保存、执行 SQL 语句和 SQL 脚本功能； (3)具备复制、编辑现有数据库对象功能； (4)具备关键词显示标记、动态语法提示的 SQL 编辑器功能
30.	功能要求		*用户、角色管理工具	(1)支持创建、修改、删除用户的功能； (2)提供定义用户的功能； (3)支持创建、修改、删除角色的功能，且提供用户自定义角色的功能
31.	功能要求		*SQL 执行计划查看工具	(1)提供与数据库管理系统进行 SQL 交互的工具，方便运维工作； (2)支持查看 SQL 语句查询执行计划与统计信息
32.	功能要求		*数据库对象工具	(1)支持创建、修改、删除表的功能，支持定义表结构、约束、存储配置管理的功能； (2)支持创建、修改、删除索引的功能，支持定义索引结构、类型、存储配置管理的功能； (3)支持创建、修改、删除视图的功能，支持视图定义的功能； (4)支持创建、修改、删除约束的功能，支持约束定义的功能
33.	功能要求		*导入导出工具	(1)支持导出不同格式，可以将不同格式数据导入到数据库中； (2)支持不同级别和不同数据库对象的导入/导出功能； (3)支持从文本文件或者其他上游数据源将数据导入； (4)支持 SQL 脚本进行导入导出

序号	指标分类	一级指标	二级指标	指标要求
34.	功能要求		*数据库运维工具	(1)支持数据库、数据库存储对象结构、数据、统计信息更新维护； (2)支持数据库创建、数据库修改、数据库删除、数据库模板维护； (3)支持数据库任务自动化调度作业管理； (4)支持图形化展示数据库管理的各种元数据界面，展示的内容具有层次性，包括模式、非模式数据字典信息
35.	功能要求	*图形化管理	*图形化的开发工具	厂商提供图形化的开发工具
36.	功能要求		*图形化运维工具	厂商提供图形化的运维工具
37.	可靠性要求	*稳定运行	*稳定运行	(1)支持连续稳定运行； (2)支持数据库管理系统运行风险的报警能力
38.	可靠性要求	*故障切换	*快速切换	支持快速切换，在主数据库出现故障时，能够快速切换到备用数据库，保障业务正常运行
39.	可靠性要求		*恢复无断点	支持无断点恢复能力
40.	可靠性要求	*容灾能力	*主备备份	(1)支持多副本，支持主副本与从副本之间的数据同步，最低时延由生产厂商提供； (2)提供基于主机的数据库复制技术，包括基于日志的备用数据库远程数据库备份技术，并具备数据副本间的复制能力
41.	可靠性要求		*实例容灾	(1)在任意数据库实例出现故障时，集群内服务正常运行，数据不丢失，集群整体业务可用； (2)在实例故障、节点故障等单数据库实例故障时，RPO 时间等于 0，RTO 时间小于 30s
42.	可靠性要求		*容灾部署	(1)提供远程容灾部署与管理功能； (2)提供生产中心与备份中心之间的容灾部署与管理功能
43.	可靠性要求		*同城容灾	(1)支持同城双中心部署，当主中心故障时，业务切换到备中心； (2)由于网络、供电等原因造成的可用区级故障，触发集群计划外停机，在同城多可用区场景下，RPO 时间等于 0，RTO 时间小于 1 分钟
44.	可靠性要求	*容错性	*服务端编程稳定性	支持当用户自定义的存储过程、函数运行异常时，数据库稳定运行
45.	可靠		*网络容错	支持网络中断时，保障事务一致性

序号	指标分类	一级指标	二级指标	指标要求
	性要求			
46.	可靠性要求		*检测报警	(1)支持数据库实例启动时错误检测能力； (2)支持加载不同文件格式、不同大小数据出现错误时的故障检测和处理能力； (3)支持数据库备份执行过程中发生故障时报错或者报警能力； (4)支持数据库恢复发生故障时报错或者报警能力
47.	可靠性要求		*故障恢复	(1)系统故障重启后能正常运行且支持数据一致性； (2)支持完全媒体故障恢复的能力； (3)提供基于时间点故障恢复功能
48.	可靠性要求		*不同级别故障可恢复	支持数据库事务故障、系统故障、存储媒体故障不同级别的可恢复能力
49.	兼容要求	*硬件兼容	*硬件平台兼容	(1)同源支持以下至少三种 CPU 平台架构： 1. ARM； 2. LoongArch； 3. MIPS； 4. SW64； 5. x86； (2)支持 SMP 和 NUMA 的运行环境
50.	兼容要求	*标准兼容	*ODBC	支持 ODBC
51.	兼容要求		*JDBC	支持 JDBC
52.	服务要求	*交付方式	*交付方式	以光盘、便携式移动设备、镜像文件、在线下载等交付方式提供产品交付物
53.	服务要求	*服务周期	*产品维护周期	产品自发布之日起至产品停止功能升级（包含不限于新特性、新硬件支持、问题修复、安全补丁等）之日止≥5 年
54.	服务要求		*产品延伸服务周期	产品停止功能升级之日起至产品停止功能维护（包括问题修复、安全补丁等）之日止≥4 年
55.	服务要求		*产品延伸安全服务周期	产品功能维护停止之日起至产品停止安全维护（包括中高风险漏洞修复）之日止≥2 年
56.	服务要求		*售后服务最小保障期	自销售之日起，产品售后服务周期≥6 年
57.	服务要求	*供应链与服务保障	*供应链与服务保障基础要求	(1)提供多种形式支持服务，包含电话、电子邮件、远程连接等； (2)提供技术支持服务，支持同城 4h、异地 12h 响应要求，两个工作日解决问题，对于未能解决的问题和故障提供可行的升级方案；

序号	指标分类	一级指标	二级指标	指标要求
				(3)提供培训材料、产品手册、培训视频等培训相关内容； (4)建立全国技术服务体系和服务团队，符合专业服务体系标准要求，提供原厂中文服务； (5)服务周期内支持版本免费升级； (6)开源产品对获得的社区源代码进行安全性和知识产权审查与管理； (7)提供数据库参数、慢 SQL 语句的性能优化指南，包含性能优化的具体措施、技巧、案例及建议等
58.	安全要求	*基本要求	*基本要求	数据库应当符合安全可靠测评要求
59.	安全要求	*基础安全	*漏洞管理	建立漏洞管理机制，及时通过邮件、网站等方式将安全漏洞告知用户，并提供安全补丁对漏洞进行修复
60.	安全要求		*身份鉴别及访问控制	提供身份鉴别及访问控制，加解密的密码要求符合 GM/T0028 的相关规定

3. 操作系统采购需求标准

3.1.桌面操作系统

序号	指标分类	一级指标	二级指标	指标要求
1.	功能要求	*操作系统支持多 CPU 架构	*同源兼容多 CPU 平台架构	操作系统同源兼容 ARM、LoongArch、MIPS、SW64、x86 等平台架构的 CPU
2.	功能要求	*操作系统支持 CPU 内置功能	*多核支持	操作系统支持双核及多核处理器，支持核间负载均衡、线程绑定，并提供系统多核访问及调度接口
3.	功能要求		*CPU 虚拟化支持	操作系统支持 CPU 虚拟化技术
4.	功能要求		*动态调节 CPU 运行频率	操作系统根据负载情况，自动调节 CPU 的运行频率
5.	功能要求		*支持 CPU 运行时低功耗状态切换	操作系统根据负载的情况，自动切换 CPU 的低功耗状态
6.	功能要求		*支持 CPU 内置安全功能	操作系统支持 CPU 硬件密码运算与随机数生成等功能，并提供标准接口供应用程序调用
7.	功能要求	*安装部署	*安装方式	操作系统支持光盘、USB 闪存盘和网络等安装方式

序号	指标分类	一级指标	二级指标	指标要求
8.	功能要求		*安装过程配置	操作系统支持安装界面文种设置，默认为简化汉字方式显示，提供时区设置、计算机名设置等
9.	功能要求		*硬盘分区	操作系统支持整个硬盘自动分区、自定义分区，支持逻辑分区配置（如 LVM），支持创建备份分区；自定义分区时能自动检测分区设置的合规性，删除已有分区或格式化硬盘提示告警信息
10.	功能要求		*双硬盘安装	当计算机同时存在固态硬盘和机械硬盘时，自动分区优先将系统盘（或分区）设置在固态硬盘，优先将数据盘（或分区）设置在机械硬盘
11.	功能要求		*多系统安装	操作系统能够识别已安装的其他系统，可自动复用引导分区等，并实现多系统引导
12.	功能要求		*加密	操作系统应提供基于分区的用户数据加密功能，保护用户存储区数据安全
13.	功能要求		*初始化备份	操作系统应提供用户备份初始系统环境的功能
14.	功能要求		*保留用户数据	用户重装操作系统时提供保留用户数据的功能
15.	功能要求	*系统引导	*引导模式	操作系统应支持 UEFI2.0 及以上规范固件引导： (1)当计算机以 UEFI 模式启动安装时，安装程序应分配 ESP，并在 ESP 中放置启动引导文件，使操作系统能以 UEFI 模式引导； (2)当计算机固件不支持 UEFI 模式时，安装程序根据计算机固件提供的引导方式，安装系统引导代码或配置系统引导选单，使安装完的系统可以正常引导
16.	功能要求		*引导修复	安装程序提供系统引导修复功能，当已安装的操作系统引导被破坏时，可重建系统引导
17.	功能要求	*其他安装要求	*图形化显示	操作系统应提供安装过程图形化显示
18.	功能要求		*安装提示	操作系统在安装执行前明确提示用户可能会删除已有数据，并提供退出或取消功能；当用户取消安装时，不改变硬盘上已有数据；如用户自定义的某些配置可能会影响后续的正常使用，予以明确提示
19.	功能要求		*分辨率自适应	操作系统安装完成后自动适配显示器最佳分辨率
20.	功能要求	*系统内核	*内核要求	(1)若操作系统是基于 Linux 内核的微型计算机操作系统应兼容 5.4 版内核主要功能，包括进程管理、内存管理、任务调度、中断处理、并发与同步处理等；

序号	指标分类	一级指标	二级指标	指标要求
				(2)若操作系统属于其他类型内核不做要求
21.	功能要求	*进程管理	*进程调度	操作系统支持进程创建、分组、删除及进程信息获取
22.	功能要求		*优先级设置	操作系统支持进程优先级设置，包括优先级范围设置、优先级调度策略设置等
23.	功能要求		*地址映射	操作系统支持进程内存地址的正向映射和反向映射
24.	功能要求	*内存管理	*内存地址管理	操作系统支持基础连续虚拟地址、连续物理地址的申请、回收和释放
25.	功能要求		*内存管理单元	操作系统支持内存管理单元，通过页表映射实现虚拟地址和物理地址的映射关系
26.	功能要求		*buddy 分配器	(1)若操作系统基于 Linux 内核，支持 buddy 分配器，支持 slob、slub 或 slab 分配器； (2)若操作系统属于其他类型内核不做要求
27.	功能要求		*DMA 内存	操作系统支持 DMA 内存的申请和释放，包括流式 DMA、一致性 DMA 以及大内存 DMA
28.	功能要求		*内存 zone 管理	(1)若操作系统基于 Linux 内核，操作系统支持内存 zone 管理； (2)若操作系统属于其他类型内核不做要求
29.	功能要求		*内存分配方式	操作系统支持不交换硬盘的内存分配方式
30.	功能要求	*任务调度	*上下文切换	操作系统支持进程上下文切换
31.	功能要求		*进程负载均衡	操作系统支持进程负载均衡调度方式
32.	功能要求		*调度方式	操作系统支持进程基于时间片的调度方式
33.	功能要求		*抢占调度方式	操作系统支持进程抢占调度方式
34.	功能要求	*中断处理	*中断处理	操作系统支持硬件中断号和软件中断号的映射、注册和处理；支持高精度时钟中断、类软中断和类 tasklet 下半部中断处理；支持中断使能、屏蔽、亲和力处理以及中断抢占；支持中断工作队列处理，包括工作队列创建、初始化、调度和回收等
35.	功能要求	*并发与同步处理	*并发同步处理	操作系统支持自旋锁、信号量、互斥体等原子操作；支持读写锁、类 RCU 原子操作；支持内存屏障操作
36.	功能要求	*中文支持要求	*字符编码	操作系统符合 GB 18030 的要求
37.	功能要求		*字库	操作系统提供符合 GB 18030 标准的字库，至少包括宋体、仿宋体、黑体、楷体及小标宋

序号	指标分类	一级指标	二级指标	指标要求
				体在内的 5 种字库；支持曲线字库，可无级放缩字形大小，以适应不同分辨率的输出设备，输出字形应字形正确，字体规范；支持用户扩展安装字库
38.	功能要求		*输入法	操作系统应内置输入法框架;至少提供一种音码和一种型码输入法；支持 GB 18030 中已编码的语言文字输入法的安装使用
39.	功能要求		*输入法标准	操作系统提供的通用键盘输入法应符合 GB/T 19246—2003 要求；如提供手写输入法，应符合 GB/T 18790—2010 要求；如提供语音输入法，应符合 GB/T 21023—2007 要求
40.	功能要求		*输出	系统配置的字库能被工具或软件正常调用打印和显示
41.	功能要求		*表示	操作系统提供中文界面显示,提供符合要求的日期、星期、上下午、时间、货币、数字等显示及表示方式
42.	功能要求	*系统管理要求	*系统信息	操作系统提供系统信息查看工具,支持用户查看系统版本、内核版本、内存容量、CPU 型号等信息
43.	功能要求		*系统资源管理	操作系统提供系统资源管理工具并图形化显示进程信息、资源信息、文件资源信息等
44.	功能要求		*硬盘管理	操作系统提供硬盘管理工具,显示硬盘容量及硬盘信息，支持新建和删除硬盘分区，分区支持 EXT3、EXT4、FAT32、NTFS、XFS、exFAT、Btrfs 等文件系统格式
45.	功能要求		*设备信息	操作系统提供设备信息工具，显示 CPU、内存、主板、存储、网卡、声卡、电源、USB、蓝牙等参数信息，显示硬件信息、计算机型号和操作系统信息、设备驱动状态（启用或禁用），并支持设备启用、禁用状态设置
46.	功能要求		*文件管理器	操作系统支持按文件名、文件类型、文件修改时间、文件大小排序显示文件;支持文本文件、图片文件和视频文件首帧的预览;显示当前用户的主目录、桌面、文档、下载、回收站等文件资源；支持对光驱、闪存盘的访问；支持对网络资源的访问，包括 SMB、FTP、NFS 等协议下的网络资源;支持通过地址栏输入绝对路径定位文件夹;支持文件按照列表显示或网格图标显示；支持新建文件、文件夹和快捷方式，并支持扩展新建的文件类型；支持全选当前文件夹所有文件，支持文件多选、反选；支持复制、粘贴、删除、剪切、重命名、压缩等

序号	指标分类	一级指标	二级指标	指标要求
				文件操作；支持选择文件打开方式，可以使用默认用程序打开，并支持修改默认用程序；支持按文件名、修改时间、文件大小等搜索
47.	功能要求		*本地帐户管理	操作系统提供图形管理界面，支持帐户和用户组管理，支持口令、头像、权限设置，支持口令修改，支持重设管理帐户口令
48.	功能要求		*登录管理	操作系统支持本地帐户、LDAP 帐户鉴别登录，提供口令、指纹、人脸、U-Key 等多种鉴别方式登录，支持本地帐户免口令登录和自动登录
49.	功能要求		*鼠标管理	操作系统提供图形化鼠标管理工具；支持鼠标灵敏度、滚轮方向的设置与测试；支持左右手习惯设置；对于带触控板的微型计算机，应具有触控板管理功能，包括启动与禁止及相应的防误触等功能
50.	功能要求		*键盘管理	操作系统提供键盘图形化管理工具；支持重复键延时及速度设置；支持数字键盘、大写锁定提示
51.	功能要求		*显示管理	操作系统支持屏幕分辨率设置；支持屏幕刷新率设置；支持屏幕亮度设置； 支持屏幕显示冷暖色温手动、自动调节；支持多个屏幕以复制、扩展、单独方式输出显示，支持多个屏幕显示位置设置，支持各屏幕显示方向独立设置；支持 4K 高分辨率屏幕显示，支持手动和自适应匹配设置窗口等比缩放显示；支持超宽屏显示，如：21:9、32:9 的显示器；支持触屏功能，包括选择、点击、双击、滚动等操作；支持登录界面、锁屏界面、系统桌面的背景图片设置；支持屏幕保护定时设置和帐户口令鉴权恢复
52.	功能要求		*声音管理	操作系统支持输出音量大小设置、静音设置；支持系统默认音效配置；支持输入输出设备配置；支持输入噪音抑制开关设置；支持输出音量增强开关设置；支持输出声道左右平衡设置
53.	功能要求		*快捷键管理	操作系统支持预先定义系统快捷键；支持自定义快捷键
54.	功能要求		*时间日期管理	操作系统支持图形化显示；支持系统日期、时间设置；支持时区设置；支持网络时钟同步设置
55.	功能要求		*电源管理	操作系统支持空闲时显示器转入待机的时间设置；支持空闲时计算机转入屏幕保护的时间设置；支持屏幕显示亮度设置；便携式计算机使用时支持高性能、平衡、节能等模式设置

序号	指标分类	一级指标	二级指标	指标要求
56.	功能要求		*输入法管理	操作系统支持添加和删除输入法;支持快捷键设置，包括输入法启动、输入法激活/非激活切换、顺序切换等；支持多种输入法共存
57.	功能要求		*默认登录语言	按照安装时选择的文种类型作为初次登录系统文种
58.	功能要求		*打印机管理	操作系统支持添加和删除打印机;支持添加本地打印机、网络打印机及共享打印机；支持打印机共享；支持查看打印机列表；支持任务队列管理，包括取消、暂停、挂起；支持页面设置；提供接口查询打印机打印状态，包括指定文件打印成功的页数、份数、页码及打印失败的文件名和页码等信息
59.	功能要求		*外设管控	操作系统支持动态显示未授权设备信息;支持接口控制、设备控制、权限控制等（接口包括USB、蓝牙、网络接口等；设备包括打印机、摄录设备、USB 存储设备等；权限包括读、写、执行等）；支持按设备类型、设备 ID、接口等配置设备接入黑白名单策略;提供完整的连接记录，记录可追溯
60.	功能要求		*隐私文件保护	操作系统提供基于独立口令和密钥保护的文件保险箱;支持口令和透明加解密鉴权访问文件保险箱内的文件和文件夹;支持手动上锁文件保险箱；支持通过密钥找回口令
61.	功能要求		*网络管理	支持图形化显示；支持 DNS 设置；支持 IPV4/IPV6 地址配置；支持自动获取网络地址；支持网关设置；支持手动/自动设置网络代理服务器，支持 HTTP、HTTPS、FTP、SOCKS 等多种协议；支持无线网络管理，包括连接或断开网络、配置口令、手动刷新无线热点列表等；支持个人热点共享，包括有线、无线网络生成的网络热点；支持 L2TP、PPTP、OpenVPN、StrongSwan 类型的 VPN 连接，支持新增、导入、编辑和删除连接配置，支持启用或禁用 VPN 自动连接
62.	功能要求		*默认应用程序管理	操作系统提供默认用程序管理工具,支持预先定义和修改指定用类型的默认程序，包括图片、文本、音视频、网页、邮件
63.	功能要求		*通知管理	操作系统任务栏提供通知中心图标,并显示消息提醒;系统和应用使用通知接口发送通知消息；支持对通知消息的管理，包括显示、删除、清理等
64.	功能要求		*主题管理	操作系统提供图形化主题管理工具;支持以深色、浅色和昼夜切换自动配色方式显示系统图

序号	指标分类	一级指标	二级指标	指标要求
				形化界面；支持系统主题颜色设置；支持系统图标主题设置；支持系统光标主题设置
65.	功能要求	*图形化要求	*用户操作界面	操作系统提供图形化操作界面
66.	功能要求		*桌面图标	操作系统默认提供我的系统、个人文档、回收站等图标
67.	功能要求		*桌面图标管理	操作系统提供回收站工具，可收集要删除的文件和文件夹，并支持右键清空操作；支持应用程序快捷方式与文件共存；支持右键选单进行复制、剪切和粘贴文件操作；支持文件图标拖拽、摆放；支持图标名称修改；支持按照文件类别显示文件图标
68.	功能要求		*桌面快捷选单	操作系统支持桌面图标按照网格排列；支持右键选单新建纯文本；支持右键选单新建文件夹；支持右键选单选择图标排列顺序，排序可按名称、类型、修改时间、文件大小
69.	功能要求		*起始选单	操作系统支持分类显示系统已安装应用；支持创建应用的快捷方式到桌面；支持添加应用访问快捷方式到任务栏；支持多种方式搜索内容，支持拼音搜索、模糊搜索快捷查找系统应用；支持新安装应用与应用列表中其他应用以明显方式区分，包括突出显示、增加标识或单独分类；包含电源操作按钮，并可触发系统退出界面；包含直接进入控制系统或配置系统的功能入口或应用图标
70.	功能要求		*任务栏	操作系统应提供图形化任务管理工具栏，任务栏中应该包括快速启动栏、通知栏；提供快速启动应用程序区，可以添加或删除应用启动快捷方式；提供系统通知栏，显示网络、声音、电源、USB 设备等，支持应用程序（如输入法等）的状态信息；提供显示桌面功能，支持最小化当前所有窗口，在有活动窗口的情况下快速切换成只显示用户桌面；对已切换成只显示用户桌面的状态，可以快速切换回活动窗口状态；直观区分任务栏应用运行与未运行的状态；支持任务栏隐藏；支持任务栏位置调整
71.	功能要求		*桌面工作区	操作系统支持多工作区，支持应用跨工作区移动；可配置工作区数量；可通过快捷键切换工作区
72.	功能要求		*系统退出	操作系统退出界面应为模态或全屏界面，提供选择关机、重启、锁定、注销、休眠、待机等六种操作
73.	功能		*窗口管理器	操作系统支持对窗口的操作，如最小化、最大

序号	指标分类	一级指标	二级指标	指标要求
	要求			化、移动、改变大小、总是置顶或在最前端、关闭；提供窗口显示最小化、最大化和关闭按钮；提供窗口标题，显示窗口名称，并区别显示选中和未选中窗口；窗口可以在不同工作区中移动；提供窗口防呆功能，防止窗口完全移出桌面范围内；提供窗口切换功能，通过快捷键可在打开的窗口中按一定顺序进行快速切换；提供多任务视图功能，可以预览当前工作区内已打开的所有窗口；支持一键操作移开桌面所有窗口，显示桌面；提供多窗口分屏功能，支持屏幕分割显示各窗口，支持同时调整窗口尺寸
74.	功能要求		*图形特效	操作系统窗口显示支持模糊透明特效，当支持透明效果的窗口与其他窗口重叠时，前置窗口颜色能随背景窗口颜色的融合发生变化；提供窗口外观装饰效果设置，如边框、阴影、模糊、透明度、圆角等，且透明度可调节
75.	功能要求	*常用软件支持	*应用软件安全要求	操作系统预装应用软件应进行签名认证，确保应用软件的安全性、稳定性、可靠性
76.	功能要求		*压缩工具	操作系统提供压缩解压缩工具，支持 zip、7z、tar、tar.7z、tar.bz2、tar.gz 等压缩格式新建、打开、解压操作，以及对压缩文件中所含文件进行添加、删除、重命名等操作；支持解压 rar 格式文件；支持对压缩包进行加解密
77.	功能要求		*音频播放工具	操作系统提供音频播放工具，支持 MP3、OGG、WAV 等音频格式文件；支持播放本地音频文件；支持本地音乐文件搜索功能；支持播放控制，可设置播放模式
78.	功能要求		*音频录制工具	操作系统提供音频录制工具，支持系统播放和传声器输入的音频录制为文件；支持录制音频过程中的录制、暂停、续录和停止等操作
79.	功能要求		*视频播放工具	操作系统提供视频播放工具，支持 MKV、OGG 等封装格式的视频文件；支持播放本地视频文件；支持自动加载本地字幕；支持播放控制功能；提供软件解码与硬件编解码切换选项，如硬件支持编解码，应优先使用
80.	功能要求		*视频录制工具	操作系统提供视频录制工具，支持通过摄像头等设备拍摄图片和录制音视频文件；拍摄照片时，支持设置构图网格、快门音效、多张连拍、延时拍摄、镜像拍摄和图像分辨率；录制音视频时，支持延时录制
81.	功能要求		*光盘刻录管理工具	操作系统提供光盘刻录管理工具，支持 CD-R、CD-RW、DVD-R、DVD-RW、DVD+R、

序号	指标分类	一级指标	二级指标	指标要求
				DVD+RW 格式的光盘；支持将光盘复制为镜像文件保存到另一张光盘；支持将光盘镜像文件刻录到光盘；支持 ISO9660、UDF 格式光盘挂载、读取；支持 ISO9660 格式光盘追加刻录；支持检查光盘数据完整性
82.	功能要求		*截图录屏	操作系统提供截图录屏工具，支持系统截图和录屏；支持延时捕捉屏幕图像设置；支持录制光标移动、鼠标点击、键盘操作痕迹、系统音频、传声器输入、摄像头画中画内容；支持多种截图区域，包括全屏、程序窗口和自选区域；支持多种保存选项，包括保存到系统默认文件夹、桌面、指定存储路径、剪贴板；系统截图支持保存为 PNG、JPG、BMP 等格式，录屏支持保存为 GIF、MP4、MKV 等格式
83.	功能要求		*图像查看工具	操作系统提供图像查看工具，支持查看图像文件，支持 PNG、JPEG、TIFF、GIF、BMP 等图像格式；支持显示图像文件的基本信息，包括文件大小、图像格式、宽度和高度等；支持对图像文件的操作，包括放大、缩小、旋转、打印等
84.	功能要求		*文件扫描工具	操作系统提供文件扫描工具，支持扫描文件类型设置，包括 PNG、JPEG、TIFF、BMP、PDF 等；支持扫描颜色设置，包括彩色、灰度；支持扫描分辨率、幅面设置
85.	功能要求		*浏览器	操作系统提供浏览器，支持 HTML4、HTML5、ECMAScript、CSS 等标准；支持符合国家密码管理要求的商用密码算法；支持国家电子认证根 CA 签发的符合相关要求的 CA 机构证书；支持符合 GB/T 38636—2020 的 TLCP
86.	功能要求		*文件共享	操作系统提供文件共享工具，支持按用户身份进行读写权限设置
87.	功能要求	*开发环境	*开发环境	操作系统通过内置、软件仓库或附加光盘等方式提供如 Qt、Eclipse、VSCode 等集成开发环境
88.	功能要求		*开发库	操作系统通过内置、软件仓库或附加光盘等方式提供如 GNU C、GNU C++、Java、Qt 、Gtk+、Cairo、OpenGL、Perl、Python、Ruby、Rust、Golang、JS 等开发库
89.	功能要求		*编译开发工具	操作系统通过内置、软件仓库或附加光盘等方式提供如 GCC、G++、Binutils、GDB、Make、CMake 等语言编译器
90.	功能		*文本编辑工	操作系统通过内置、软件仓库或附加光盘等方

序号	指标分类	一级指标	二级指标	指标要求
	要求		具	式提供如 Emacs、Vim 等。
91.	功能要求	*开发支持	*开发文档	操作系统应内置或通过官方网站、社区等提供中文开发文档，包括：软件开发参考文档；驱动开发参考文档；应用移植开发文档；API 文档
92.	兼容性要求	*运行环境兼容	*版本兼容	操作系统基础运行库或开发环境向后（向下）兼容，即系统版本升级后，能兼容上一版本所运行的软件与设备；系统主版本兼容维护时间自发布之日起不低于 5 年，包括但不限于安全修复、功能升级、新硬件支持等；支持以增量升级包的方式实现版本更新
93.	兼容性要求		*文件系统层次结构	供应商应给出长期兼容支持的文件系统层次结构
94.	兼容性要求		*运行库	供应商应给出长期兼容支持的运行库
95.	兼容性要求		*命令	供应商应给出长期兼容支持的常用命令
96.	兼容性要求	*软件包	*软件包管理	操作系统支持图形化方式下载、安装和卸载软件包；显示已安装软件包的描述和包含的文件；支持安装时优先自动进行缺失依赖软件包的下载和安装；自动检测本地安装包，当发现安装包未经签名认证时自动告警；在连接软件仓库/应用商店时（含局域网、广域网）能自动搜索并下载依赖的软件包
97.	兼容性要求	*硬件兼容（整机）	*微型计算机兼容清单	供应商提供兼容的台式微型计算机品牌及型号清单，且至少兼容一款产品
98.	兼容性要求		*便携式微型计算机兼容清单	供应商提供兼容的便携式微型计算机品牌及型号清单，且至少兼容一款产品
99.	兼容性要求	*硬件兼容（部件）	*固件	供应商提供兼容的固件品牌及型号清单，且至少兼容一款产品
100.	兼容性要求		*显卡	供应商提供兼容的显卡品牌及型号清单，且至少兼容一款产品
101.	兼容性要求		*网卡	供应商提供兼容的有线、无线网卡品牌及型号清单，且至少兼容一款产品
102.	兼容		*蓝牙	供应商提供兼容的蓝牙设备品牌及型号清单，

序号	指标分类	一级指标	二级指标	指标要求
	性要求			且至少兼容一款产品
103.	兼容性要求		*显示设备	供应商提供兼容的显示设备品牌及型号清单，且至少兼容一款产品
104.	兼容性要求		*生物特征	供应商提供兼容的生物识别设备（指纹、人脸）品牌及型号清单，且至少兼容一款产品
105.	兼容性要求	*硬件兼容（外设）	*打印机	供应商提供兼容的打印机品牌及型号清单，且至少兼容一款产品
106.	兼容性要求		*扫描仪	供应商提供兼容的扫描仪品牌及型号清单，且至少兼容一款产品
107.	兼容性要求		*摄录设备	供应商提供兼容的摄录设备品牌及型号清单，且至少兼容一款产品
108.	兼容性要求		*存储设备	供应商提供兼容 USB2.0，3.0，3.1 的 U 盘和移动硬盘品牌及型号清单，且至少兼容一款产品
109.	兼容性要求		*主流蓝牙设备	供应商提供兼容的蓝牙鼠标、键盘、音响等品牌及型号清单，且至少兼容一款产品
110.	兼容性要求		*主流 USB 外设	供应商提供兼容的 USB 设备，如 USB 鼠标、键盘、音响、网卡等品牌及型号清单，且至少兼容一款产品
111.	兼容性要求	*软件兼容（日常办公）	*办公软件	供应商提供兼容的办公软件品牌及版本清单，且至少兼容一款产品
112.	兼容性要求		*版式软件	供应商提供兼容的版式软件品牌及版本清单，且至少兼容一款产品
113.	兼容性要求		*签名软件	供应商提供兼容的电子签名、电子签章、云签章、key 签署等签名软件的品牌及版本清单，且至少兼容一款产品
114.	兼容性要求	*软件兼容（安全防护）	*杀毒软件	供应商提供兼容的杀毒软件的品牌及版本清单，且至少兼容一款产品
115.	兼容性要求		*身份鉴别系统	供应商提供兼容的通过指纹、人脸识别、Ukey 等方式对使用者身份进行验证的系统品牌及版本清单，且至少兼容一款产品
116.	兼容性要		*日志管理	供应商提供兼容的日志管理软件品牌及版本清单，且至少兼容一款产品

序号	指标分类	一级指标	二级指标	指标要求
	求			
117.	兼容性要求		*防火墙	供应商提供兼容的网络防护、安全管理等软件的品牌及版本清单，且至少兼容一款产品
118.	兼容性要求	*软件兼容（网络应用）	*网络会议	供应商提供兼容的网络会议软件的品牌及版本清单，且至少兼容一款产品
119.	兼容性要求		*浏览器	供应商提供兼容的浏览器的品牌及版本清单，且至少兼容一款产品
120.	兼容性要求		*新闻信息	供应商提供兼容的新闻信息类软件的品牌及版本清单，且至少兼容一款产品
121.	兼容性要求		*社交软件	供应商提供兼容的社交软件的品牌及版本清单，且至少兼容一款产品
122.	兼容性要求	*软件兼容（多媒体）	*图形图像	供应商提供兼容的图像查看、图像编辑的品牌及版本清单，且至少兼容一款产品
123.	兼容性要求		*媒体播放	供应商提供兼容的媒体播放类软件品牌及版本清单，且至少兼容一款产品
124.	兼容性要求		*音乐电台	供应商提供兼容的多媒体类软件品牌及版本清单，且至少兼容一款产品
125.	易用性要求	*便捷使用	*帮助提示	操作系统提供内置系统和应用中文图文用户手册，包括使用说明、示例、常见故障处理等；对需要补充解释的部分，以合适方式提供中文提示
126.	易用性要求		*快捷键	操作系统支持以下快捷键：<Super> 开始选单 <Alt>+<Tab> 遍历窗口<Shift>+<Alt>+<Tab> 反向遍历窗口<Alt>+<F4> 关闭当前窗口 <Ctrl>+<A> 全选<Ctrl>+<X> 剪切 <Ctrl>+<C> 复制<Ctrl>+<V> 粘贴 <Ctrl>+<Space> 开启/关闭输入法 <Ctrl>+<Shift> 切换输入法<Super>+<L> 桌面锁定<Super>+<D> 显示桌面<Super>+<E> 打开文件管理器<Ctrl>+<Alt>+<Delete> 退出界面
127.	可靠性要求	*系统稳定性	*操作系统连续运行 72 小时	操作系统在 CPU 占用大于等于 80%，或内存占用大于等于 80%压力情况下，连续运行 72 小时无故障
128.	可靠	*检查修复	*系统修复	操作系统提供文件系统检查与修复功能，能自

序号	指标分类	一级指标	二级指标	指标要求
	性要求			动修复文件系统错误或以显式方式提示用户进行手动文件系统修复
129.	可靠性要求	*备份恢复	*备份还原	操作系统提供备份还原功能：支持系统的备份和还原；支持全盘备份到外部存储设备；支持还原到指定备份点；支持保留用户数据的系统还原；支持系统无法正常进入状态时，可对系统进行还原
130.	可维护性要求	*系统维护	* 日志管理	操作系统提供日志管理工具：支持图形化显示；支持对系统日志信息的显示和刷新；支持对日志文件的查找和导出；支持对特定时间段内的日志进行筛选；支持系统日志定期清除功能
131.	可维护性要求		*系统升级	操作系统支持系统增量升级功能，对系统部件、安全补丁等升级；支持在线升级和离线升级；升级不得修改破坏用户数据；升级不得影响原有软硬件兼容性；提供升级回退机制，能卸载已升级的软件包，恢复系统原有状态；如升级为不可回退，则系统升级前以显式的提示告知用户
132.	服务要求	*交付方式	*交付方式	操作系统支持光盘、USB 闪存盘、镜像文件（下载）等交付方式
133.	服务要求	*产品维护服务周期	*产品维护周期	产品自发布之日起至产品停止功能升级（包含不限于新特性、新硬件支持、问题修复、安全补丁等）之日止≥5 年
134.	服务要求		*产品延伸服务周期	产品停止功能升级之日起至产品停止功能维护（包括问题修复、安全补丁等）之日止≥4 年
135.	服务要求		*产品延伸安全服务周期	产品功能维护停止之日起至产品停止安全维护（包括中高风险漏洞修复）之日止≥2 年
136.	服务要求		*产品售后服务周期	≥6 年
137.	服务要求	*售后服务	*原厂服务	服务由操作系统厂商的正式员工提供，不由代理商提供
138.	服务要求		*服务热线电话	操作系统厂商为最终用户提供工作日每日不少于 8h（应覆盖一般工作时间，具体时间由企业标准给出）中文技术服务热线
139.	服务要求		*技术服务标准	操作系统厂商提供工作日每日不少于 8h 技术支持服务
140.	服务要求		*技术服务时效	操作系统厂商满足同城 4h、异地 12h 响应要求，两个工作日解决问题，对于未能解决的问题和故障提供可行的升级方案
141.	服务要求		*技术服务保障	发生非人为因素故障，在七日内由操作系统厂商原厂人员免费对产品进行补充或更换
142.	服务	*交付与安	*配套资料	操作系统厂商交付产品时提供配套的技术资

序号	指标分类	一级指标	二级指标	指标要求
	要求	装调试		料，包括但不限于系统说明文件、用户手册（用户安装、操作、维护、故障排除）等
143.	服务要求	*系统更换	*系统更换	服务期内，操作系统厂商支持版本免费更换（注：更换后不延长服务期）
144.	服务要求	*厂商能力要求	*服务团队	操作系统厂商建立全国技术服务体系和服务团队，为客户提供专业的原厂中文服务
145.	供应保障要求	*数据上行安全保障	*数据收集安全保障	除用户授权采集的信息外不采集其他数据，相关信息采集无安全风险，相关数据存储在大陆境内
146.	供应保障要求	*数据下行安全保障	*数据供给安全保障	数据供给安全保障：涉及数据下载的线上服务物理服务器不出境，包括代码仓库、系统补丁、安全补丁、服务网站等
147.	供应保障要求	*代码无风险	*代码无风险	操作系统厂商可提供源代码，源代码可供第三方机构审查，开源许可合规，代码知识产权无风险，无恶意安全漏洞或后门，代码可追溯、可重构
148.	安全要求	*基本要求	*基本要求	操作系统应当符合安全可靠测评要求
149.	安全要求	*密码算法支持	*密码算法实现	操作系统支持 GM/T 0002 、GM/T 0003 和 GM/T 0004 规定的密码算法运算
150.	安全要求		*随机数生成	随机数质量符合 GM/T 0005《随机性检测规范》或 GB/T32915《信息安全技术二元序列随机性检测方法》
151.	安全要求		*内置数字证书	操作系统内置国家电子认证根 CA 的根证书
152.	安全要求		*密码协议实现	操作系统支持符合 GB/T 38636—2020 的 TLCP
153.	安全要求	*安全管理工具	*安全管理工具	操作系统提供安全管理工具，包括帐户安全、网络防护、病毒防护、应用程序执行控制
154.	安全要求	*身份鉴别	*生物特征识别管理	操作系统支持两种及以上的生物特征类型鉴别，如指纹、人脸；支持使用生物特征进行命令行、图形化提权操作的身份鉴别；支持使用生物特征进行系统登录操作的身份鉴别；支持用户管理自己的生物特征信息
155.	安全要求		*身份鉴别服务	操作系统用户标识使用帐户名和帐户 ID，在操作系统的整个生存周期内帐户标识具有唯一性；支持配置帐户口令复杂度校验及强口令管理；支持帐户口令有效期配置；支持口令鉴别失败控制；支持口令加密算法配置，帐户口令进行加密后以不可逆的密文形式保存；支持禁止根帐户(root)远程登录设置
156.	安全要求	*访问控制	*自主访问控制	允许客体拥有者以普通帐户决定并控制对客体的访问，并阻止非授权帐户对客体的访问普

序号	指标分类	一级指标	二级指标	指标要求
				通用户缺省拥有新建、读写和删除私有目录下文件的权限；支持细粒度的自主访问控制，将访问控制的粒度控制在指定帐户，对系统中的每一个客体，实现由客体拥有者以指定帐户方式确定其对该客体的访问权限，而其他同组帐户或非同组的帐户和用户组对该客体的访问权则由客体拥有者授予
157.	安全要求		*强制访问控制	操作系统支持对应用程序的访问控制与资源限制，包括对文件、网络等客体的访问控制；支持应用安装控制、应用执行控制
158.	安全要求		*安全审计	操作系统能对身份鉴别的使用、自主访问控制、标记和强制访问控制策略的修改等生成审计日志；审计记录包括事件类型、事件发生的日期、触发事件的帐户、事件成功或失败等字段；支持审计日志查询和导出功能设置
159.	安全要求	*防火墙工具	*基本要求	操作系统支持开启或关闭防火墙；支持添加防火墙规则，至少包括名称、协议、地址和端口；提供不同场景下的缺省防火墙配置，如公共、专用和自定义；支持不同的访问策略，包括允许、拒绝
160.	安全要求	*漏洞管理	*漏洞编号	操作系统支持漏洞编号，每个漏洞独立编号，可直接使用 NVDB、CNVD 或 CVE 编号；漏洞提醒，发现或获悉漏洞信息时，通过系统推送、电子邮件或官方网站等方式通知用户；漏洞修复，对已发现的安全漏洞通过补丁等方式对系统漏洞进行修复；漏洞列表，提供每个版本已修复的漏洞列表，并提供命令或网页等方式方便用户查询漏洞及其修复情况

3.2. 服务器操作系统

序号	指标分类	一级指标	二级指标	指标要求
1.	功能要求	*操作系统支持多 CPU 架构	*同源兼容多 CPU 平台架构	操作系统支持同源兼容 ARM、LoongArch、MIPS、SW64、x86 架构的 CPU
2.	功能要求	*操作系统支持 CPU 内置功能	*多核支持	操作系统支持双核及多核处理器，包括核间负载均衡、线程绑定等，并提供接口，通过访问接口获取运行状态和控制多核调度
3.	功能要求		*CPU 虚拟化支持	操作系统支持 CPU 虚拟化技术
4.	功能要求		*动态调节 CPU 运行频	操作系统根据负载情况，自动调节 CPU 的运行频率

			率	
5.	功能要求		*支持多 CPU	支持跨路内存访问，支持 CPU 间负载均衡，支持并优化 NUMA 体系架构
6.	功能要求		*支持 CPU 内置安全功能	操作系统支持 CPU 硬件密码运算与随机数生成等功能；提供编程接口供应用程序调用；支持通过硬件指令判别临界区冲突；支持调用 CPU 指令，实现自旋锁
7.	功能要求	*安装部署	*安装方式	操作系统支持光盘安装、USB 闪存盘安装、网络安装和无人值守安装
8.	功能要求		*安装模式	操作系统支持图形或文本安装模式
9.	功能要求		*安装过程配置	操作系统支持安装界面文种设置、逻辑分区配置（如 LVM）、自定义分区设置、安装组件设置、时区设置、键盘布局设置、初始用户设置、计算机名设置和网络设置，支持通过 USB 闪存盘等方式加载硬件驱动、支持设置加密文件系统
10.	功能要求		*系统引导	(1)操作系统应支持 UEFI2.0 及以上规范固件引导，当计算机以 UEFI 模式启动安装时，安装程序应分配 ESP，并在 ESP 中放置启动引导文件，使系统能以 UEFI 模式引导； (2)支持 bootloader 引导，支持 MBR 及 GPT
11.	功能要求		*引导修复	操作系统安装媒体提供系统引导修复功能，当已安装的系统引导被破坏时，可重建系统引导
12.	功能要求		*引导参数编辑	操作系统支持用户编辑引导参数，支持 GRUB 口令保护
13.	功能要求		*数据保护	安装程序在安装执行前明确提示用户可能会删除已有数据，并提供退出/取消功能，当用户取消安装时，不改变硬盘上已有数据
14.	功能要求		*分辨率自适应	操作系统安装完成后应自动适配显示器最佳分辨率(文本模式除外)
15.	功能要求		*安装配置正确性校验	操作系统安装和配置过程中，如用户自定义的某些配置可能会影响系统启动或正常使用，予以明确提示
16.	功能要求	*系统内核	*内核要求	(1)若操作系统是基于 Linux 内核的服务器操作系统应兼容 4.19 版内核 (2)若操作系统属于其他类型内核不做要求
17.	功能要求	*进程、线程调度	*NUMA	操作系统支持基于 NUMA 的亲和调度
18.	功能要求		*多核轮询	操作系统支持 CPU 多核轮询调度
19.	功能要求		*进程调度	操作系统具备进程优先级动态调整能力，允许在进程运行时对优先级进行调整；区分实时进程与非实时进程，分别进行调度；支持

				进程运行状态检查
20.	功能要求	*内存管理	*内存容量	操作系统支持最大内存不小于 4TB
21.	功能要求		*内存大页管理	操作系统允许应用申请内存大页降低页表转换
22.	功能要求		*NUMA	操作系统支持 NUMA 近节点优化
23.	功能要求	*存储管理	*RAID 支持	操作系统支持硬 RAID 和软 RAID，支持软 RAID 级别 0、1、5、6、10
24.	功能要求		*虚拟文件系统	操作系统支持将不同功能的外部设备抽象为统一的文件操作接口，包括存储、输入输出设备
25.	功能要求		*文件管理	操作系统支持文件存储、检索和共享
26.	功能要求		*可移动存储	操作系统支持对可移动外部存储的管理，包括启停、禁用、恢复等
27.	功能要求		*外部独立存储	操作系统支持使用外部独立存储设备
28.	功能要求		*多路径聚合	操作系统支持存储多路径聚合及 I/O 动态负载均衡
29.	功能要求		*故障检测	操作系统支持硬盘损坏或老化检测及信息收集
30.	功能要求		*虚拟内存	操作系统支持将硬盘的特定分区或文件作为虚拟扩展内存用于存放内存数据，支持虚拟内存压缩
31.	功能要求		*网络块设备挂载	操作系统支持 FCoE、iSCSI，支持将 Ceph 块设备视为常规存储设备挂载到某个目录并作为标准文件系统使用
32.	功能要求	*网络管理	*网络链路检测	操作系统支持网络链路故障检测、链路事件通知和链路状态查询
33.	功能要求		*TCP 卸载引擎	操作系统支持运行 TCP 协议卸载引擎的网卡
34.	功能要求		*网络协议	操作系统支持 IPv4、IPv6
35.	功能要求		*多网卡绑定	操作系统支持多网卡绑定
36.	功能要求	*文件系统	*文件系统支持	操作系统支持 XFS、EXT3、EXT4、NTFS、FAT32 等文件系统，支持相应格式分区创建、删除、格式化等
37.	功能要求		*日志式文件系统	操作系统支持日志式文件系统
38.	功能要求		*文件处理能力	操作系统支持最大文件不小于 4TB，最大分区与文件系统不小于 10PB，最大文件名长度不小于 255 字节

39.	功能要求		*分区大小调整	操作系统支持动态调整分区大小，对系统分区容量进行改变
40.	功能要求	*应用开发运行环境	*集成开发环境/开发框架	操作系统通过内置、软件仓库或附加光盘等方式提供开发环境，包括 Qt、Eclipse、VSCode 等
41.	功能要求		*开发工具库	操作系统通过内置、软件仓库或附加光盘等方式提供开发库，包括 GNU C、GNUC++、Java、Qt 、Gtk+、Cairo、OpenGL、Perl、Python、Ruby、Rust、Golang、JS 等
42.	功能要求		*编译器开发工具	操作系统通过内置、软件仓库或附加光盘等方式提供编译开发工具，包括 GCC、G++、Binutils、GDB、Make、CMake 等
43.	功能要求		*文本编辑工具	操作系统通过内置、软件仓库或附加光盘等方式提供文本编辑工具，包括 Emacs、Vim 等
44.	功能要求		*软件包管理	操作系统支持查询软件包描述和包含文件，以及软件包依赖；支持在安装时自动提示并下载安装缺失的依赖软件包
45.	功能要求		*开发文档	供应商应提供软件开发参考文档、驱动开发参考文档、应用移植开发文档、API 文档
46.	功能要求	*服务支持	*网络服务	操作系统支持 TCP/UDP
47.	功能要求		*网络共享	操作系统支持基于 NFS、SMB、FTP、CIFS 等协议的数据网络共享服务
48.	功能要求		*WEB 服务	操作系统支持基于 HTTP、HTTPS、FastCGI 等协议 WEB 服务
49.	功能要求		*加密传输服务	操作系统支持基于 IPSec 和 SSL 协议的隧道加密传输服务
50.	功能要求		*数字证书服务	操作系统支持基于 PKI 体系的数字证书服务
51.	功能要求		*访问控制服务	操作系统支持基于 RBAC(基于角色的访问控制)机制的访问控制服务
52.	功能要求		*网络管理服务	操作系统支持基于 SNMP、NETCONF、RESTCONF 等协议的网络管理服务
53.	功能要求		*时间同步服务	操作系统支持基于 NTP 协议网络时间同步服务
54.	功能要求		*远程连接服务	操作系统支持 RPC、rsync、SSH 等远程服务
55.	功能要求		*邮件服务	操作系统支持基于 SMTP、POP3、IMAP 等的邮件服务
56.	功能要求		*身份鉴别服务	操作系统支持基于轻量级目录访问协议的统一身份鉴别服务
57.	功能要求		*数据存储和查询服务	操作系统支持结构化和非结构化格式数据的存储和查询服务
58.	功能要求			操作系统支持块、文件、对象等类型的数据存储服务

59.	功能要求			操作系统支持 SQL、NoSQL、键值等类型的数据库
60.	功能要求		*存储服务	操作系统支持多种传输速率和存储协议的 SAN 和 NAS 存储
61.	功能要求		*集群支持	操作系统支持服务基于主备机制的分布式集群、高可用集群的部署模式
62.	功能要求			操作系统支持服务基于分布式通信协议的分布式集群、高可用集群的部署模式
63.	功能要求			操作系统支持基于虚拟路由器冗余协议的高可用集群部署模式
64.	功能要求		*分布式服务	操作系统支持基于同步、异步请求处理机制的分布式服务
65.	功能要求		*负载均衡模式	操作系统支持基于 OSI 模型的 4/7 层和链路层的负载均衡模式
66.	功能要求			操作系统支持基于不同调度算法的负载均衡模式
67.	功能要求		*高可用服务	操作系统提供对 HA 的支持，支持多种集群配置模式，包括主主模式、主备模式、N+1 模式和 N+M 模式，支持资源及节点故障检测
68.	功能要求	*虚拟化	*虚拟化部署	操作系统支持在 KVM、Xen、Hyper-V 虚拟机上安装部署操作系统
69.	功能要求		*内核虚拟化(KVM)	操作系统支持 KVM 虚拟化：对虚拟机进行启、停等管理操作；对虚拟机硬盘做快照并从快照恢复；兼容 qemu、libvirt 标准接口；支持 UEFI 或 legacy BIOS 方式启动；支持虚拟时钟 arch-timer；支持虚拟鼠标、键盘、触控板、声卡、显卡、硬盘、CDROM、串口 pty/p ipe/file 等设备；支持 Virtio 协议下的虚拟设备，包括串口、blk 驱动硬盘、SCSI 驱动硬盘、不同后端控制器类型的 Virtio 网卡(包括内核态、用户态、qemu)、GPU、vsock 设备等；支持硬盘和网卡选择类型 VF IO 设备；支持虚拟机 CPU、内存、网卡、硬盘等离线调整；支持虚拟机网卡、硬盘、USB 设备热插拔；支持 PCI/PCIE 设备直通；支持虚拟机热迁移和加密传输；支持虚拟机远程访问；支持虚拟机 CPU 和 I/O 线程绑定
70.	功能要求		*KVM 虚拟机管理	操作系统支持虚拟机对主机的访问控制；虚拟机可以拥有独立的物理资源，且各个虚拟机之间严格隔离；支持大页内存运行虚拟机；支持三种 CPU 型号模拟模式，包括直通、宿主模型、自定义；支持虚拟机资源调配控制，包括 Numa、CPU、内存、I/O、网卡；支持 CPU 拓扑模拟和透传
71.	功能	*容器	*容器虚拟化	操作系统支持 OC I；支持进程命名空间隔离

	要求			技术包括不限于 mnt、pid、 ipc、uts、user、network 等；支持在同 CPU 指令架构下的不同规格硬件上无缝分发，保障运行兼容性；支持沙箱扩展；支持面向容器的独立逻辑文件管理，具备在容器创建时指定专用根文件夹，容器内进程文件访问重定向等功能；支持日志查询功能；支持通过控制终端对容器内主进程的标准输入输出对接交互；支持通过控制终端对容器内新建进程的标准输入输出对接交互；支持容器存储卷管理（新增、删除、卷容量配置、自动回收）、卷共享；支持面向容器的网络设备资源分配和使用；支持 CN I；支持容器获取物理节点资源信息
72.	功能要求		*容器镜像和存储管理	操作系统支持容器镜像导入、导出；支持容器镜像分层保存、导入
73.	功能要求		*容器资源隔离和调配	操作系统支持容器资源在线调整，包括 CPU 资源、内存资源、I/O 资源等；支持文件配额分配、存储带宽资源使用量监控等机制，实现容器级 I/O 控制能力；支持面向容器的网络带宽调度策略，实现容器级网络带宽分配、使用量监控等机制；支持面向容器的存储空间使用监控、分配机制；支持容器 CPU 核独占；支持面向容器的 CPU 时间片资源按需划分机制；支持面向容器的内存分配和回收机制，实现内存使用量跟踪和管理；支持同一集群在线、离线业务混合部署；支持对容器的编排、负载均衡、调度等能力；支持根据容器在线与离线混合部署状态进行资源优先调度，提高计算机资源利用率
74.	易用性要求	*中文支持	*字符编码集	操作系统应符合 GB 18030 的要求
75.	易用性要求		*中文帮助文档	操作系统内置中文帮助文档
76.	易用性要求	*管理工具	*系统信息查看工具	操作系统支持查看系统版本、内核版本、内存容量、CPU 型号等信息
77.	易用性要求		*网络管理工具	操作系统支持多网口自动连接、网络地址（常被称为“ IP 地址”）设置、DNS 设置、路由设置；支持多网卡链路聚合，模式类型包括但不仅限于轮询、主备、802.3AD 动态链路聚合
78.	易用性要		*日期和时间管理工具	操作系统可设置时间同步服务器地址，支持局域网和广域网的同步设置

	求			
79.	易用性要求		*日志服务管理工具	操作系统支持收集系统日志
80.	易用性要求		*帐户管理工具	操作系统支持帐户添加、删除、属性修改等
81.	易用性要求		*用户操作审计工具	操作系统支持用户操作痕迹查询
82.	易用性要求		*存储管理工具	操作系统支持 EXT、XFS、NTFS、FAT、SWAP 等多种格式的分区管理
83.	易用性要求		*SNMP 协议工具包	操作系统支持 SNMP 设备和操作信息检索
84.	易用性要求		*文本终端连接工具	操作系统支持多终端协同管理
85.	易用性要求		*服务管理工具集	操作系统支持服务启动与停止，查看服务状态及日志，查询服务启动顺序及依赖关系
86.	易用性要求		*配置管理工具	操作系统提供配置管理工具，可以简化任务配置及服务管理
87.	易用性要求		*监控管理工具	操作系统支持监控系统资源使用情况，包含 CPU、内存、存储 I/O、网络 I/O 等
88.	易用性要求		*守护进程	操作系统支持按需启动守护进程，用户可自定义设定需求守护的进程，如遇异常可重新加载，实现应用持续运行
89.	兼容性要求	*基础组件兼容	*版本兼容	操作系统基础运行库或开发环境向后（向下）兼容，即系统版本升级后，能兼容上一版本所运行的软件与设备
90.	兼容性要求		*兼容周期	操作系统主版本兼容维护时间自发布之日起不低于 5 年，包括但不限于安全修复、功能升级、新硬件支持等
91.	兼容性要求	*运行环境	*文件系统层次结构	供应商应给出长期兼容支持的文件系统层次结构
92.	兼容性要求		*运行库	供应商应给出长期兼容支持的运行库
93.	兼容性要		*命令	供应商应给出长期兼容支持的常用命令

	求			
94.	兼容性要求	*软件兼容	*集群软件	供应商提供兼容的集群软件清单，且至少兼容一款产品
95.	兼容性要求		*虚拟化云平台	供应商提供兼容的虚拟化平台软件清单，且至少兼容三款产品
96.	兼容性要求		*容器云	供应商提供兼容的容器云软件清单，且至少兼容三款产品
97.	兼容性要求		*存储软件	供应商提供兼容的存储软件清单，且至少兼容一款产品
98.	兼容性要求		*数据库管理系统	供应商提供兼容的数据库软件清单，且至少兼容三款产品
99.	兼容性要求		*中间件	供应商提供兼容的中间件软件清单，且至少兼容三款产品
100.	兼容性要求		*运维平台	供应商提供兼容的运维平台软件清单，且至少兼容一款产品
101.	兼容性要求		*备份软件	供应商提供兼容的备份恢复软件清单，且至少兼容一款产品
102.	兼容性要求		*大数据平台	供应商提供兼容的大数据平台软件清单，且至少兼容一款产品
103.	兼容性要求		*终端防护及杀毒	供应商提供兼容的终端防护及杀毒软件清单，且至少兼容一款产品
104.	兼容性要求		*网络防护	供应商提供兼容的网络防护软件清单，且至少兼容一款产品
105.	兼容性要求		*身份认证	供应商提供兼容的身份认证软件清单，且至少兼容一款产品
106.	兼容性要求	*硬件兼容	*服务器整机	供应商提供兼容的服务器整机品牌及型号清单，且至少兼容一款产品
107.	兼容性要求		*AI 服务器	供应商提供兼容的 AI 服务器整机品牌及型号清单，且至少兼容一款产品
108.	兼容性要		*存储	供应商提供兼容的存储服务器整机品牌及型号清单，且至少兼容一款产品

	求			
109.	兼容性要求		*部件兼容	供应商提供兼容的系统总线、HBA 卡、RAID 卡、网卡、光纤卡、A I 加速卡、GPU、NPU 等品牌及型号清单
110.	可靠性要求	*稳定性	*操作系统连续运行 168 小时	操作系统高负载下连续常态运行 168 小时无故障
111.	可靠性要求	*备份还原	*备份还原	操作系统提供备份还原功能，支持生成系统状态快照及恢复系统状态
112.	可靠性要求	*内存纠错	*内存纠错	操作系统支持 DDR3、DDR4 等内存上的 ECC 查错、纠错
113.	可靠性要求	*热插拔	*硬盘热插拔	硬件支持时，操作系统支持硬盘热插拔
114.	可维护性要求	*维护工具	*远程维护	操作系统提供远程控制管理工具，支持 RDP、SSH、SPICE、VNC 等协议，方便用户进行文本或图形化形式的远程连接及维护
115.	可维护性要求		*文件完整检查	操作系统提供文件系统检查工具，对文件系统完整性进行检测和修复
116.	可维护性要求		*内核分析	操作系统提供内核性能分析工具，提供性能分析框架，支持对内核函数层面进行分析；提供内核探测工具，支持对内核及用户态程序动态追踪
117.	可维护性要求	*日志管理	*日志记录与存储	操作系统支持对安全事件的日志记录，包括帐户增删改、成功登录、失败登录、敏感服务开启关闭、配置修改等，日志信息详实，包括所属用户、访问时间、访问地址等；支持内核异常日志信息的记录和存储；支持内核崩溃转储机制，系统崩溃时可收集整个内存信息；支持配置远程日志功能，可将指定日志内容归档到日志服务器；支持对日志功能进行访问控制，防止未经授权的访问
118.	可维护性要求		*日志处理与分析	操作系统提供系统错误问题回溯分析工具，对系统崩溃问题及错误问题进行回溯；支持日志切分、一键收集、转储、同步机制
119.	可维护性要求	*脆弱性管理	*脆弱性管理	操作系统提供故障管理框架，内置故障分析专家系统，可与外部同类型系统互联；具备故障响应、故障警告功能，提供用户接口，支持故障响应、警告信息分发；支持故障管理守护进程，使用统一的传输信道或机制上报故障信息；具备硬件故障信息捕获、紧急处理功能，包括 CPU、内存及 PCIe 设备等

				硬件的故障；支持诊断/响应组件动态加载机制；提供或支持第三方远程诊断框架及调测工具集，实现远程诊断及调试断点功能；支持物理机、虚拟机中操作系统的故障恢复
120.	可维护性要求	*热补丁	*热补丁	操作系统支持对内核热补丁进行编号，每个热补丁拥有独立编号；支持增量修复以及回滚机制；提供热补丁合法性和一致性校验功能；提供热补丁管理机制和工具，功能至少覆盖补丁查询、安装、移除；提供热补丁升级和回滚系统日志，便于查询或回溯
121.	可维护性要求	*系统升级	*升级内容	操作系统支持系统增量升级功能，对系统部件、安全补丁等升级
122.	可维护性要求		*升级方式	操作系统支持在线升级和离线升级
123.	可维护性要求		*数据保护	操作系统升级不得修改破坏用户数据
124.	可维护性要求		*兼容性	操作系统升级不得影响原有软硬件兼容性，如有影响应显式的提示告知用户
125.	可维护性要求		*回退	操作系统提供升级回退机制，能卸载已升级的软件包，恢复系统原有状态，如升级为不可回退，则系统升级前以显式的提示告知用户
126.	服务要求	*交付方式	*交付方式	供应商提供光盘、USB 闪存盘、镜像文件（下载）等交付方式
127.	服务要求	*服务周期	*产品维护周期	产品自发布之日起至产品停止功能升级（包含不限于新特性、新硬件支持、问题修复、安全补丁等）之日止≥5 年
128.	服务要求		*产品延伸服务周期	产品停止功能升级之日起至产品停止功能维护（包括问题修复、安全补丁等）之日止≥5 年
129.	服务要求		*产品延伸安全服务周期	≥3 年
130.	服务要求		*售后服务最小保障期	≥8 年
131.	服务要求	*售后服务	*原厂服务	服务由操作系统厂商的正式员工提供，不由代理商提供
132.	服务要求		*服务热线电话	操作系统厂商为最终用户提供工作日每日不少于 8h（覆盖一般工作时间，具体时间由企业标准给出）中文技术服务热线
133.	服务要求		*技术服务标准	操作系统厂商提供工作日每日不少于 8h 技术支持服务
134.	服务		*技术服务时	操作系统厂商满足同城 4h、异地 12h 响要

	要求		效	求，两个工作日解决问题，对于未能解决的问题和故障提供可行的升级方案
135.	服务要求		*技术服务保障	发生非人为因素故障，在七日内由操作系统厂商原厂人员免费对产品进行补充或更换
136.	服务要求	*现场交付与安装调试	*现场安装调试	操作系统厂商提供产品安装与现场调试，并提供安装与调试所需的工具和设备
137.	服务要求		*配套资料	交付产品时操作系统厂商提供配套的技术资料，包括但不限于系统说明文件、用户手册（用户安装、操作、维护、故障排除）等
138.	服务要求	*系统更换	*系统更换	服务期内，操作系统厂商支持版本免费更换（注：更换后不延长服务期）
139.	服务要求	*厂商能力要求	*服务团队	操作系统厂商建立全国技术服务体系和服务团队，为客户提供专业的原厂中文服务
140.	供应保障要求	*数据安全保障	*数据收集安全保障	除用户授权采集的信息外不采集其他数据，相关信息采集无安全风险，相关数据存储在大陆境内
141.	供应保障要求		*数据供给安全保障	涉及数据下载的线上服务物理服务器不出境，包括代码仓库、系统补丁、安全补丁、服务网站等
142.	供应保障要求	*代码无风险	*代码无风险	操作系统厂商提供源代码，源代码可供第三方机构审查，开源许可合规，代码知识产权无风险，无恶意安全漏洞或后门，代码可追溯、可重构
143.	安全要求	*基本要求	*基本要求	操作系统应当符合安全可靠测评要求
144.	安全要求	*密码算法支持	*密码算法实现	操作系统支持 GM/T 0002 、GM/T 0003 和 GM/T 0004 规定的密码算法运算
145.	安全要求		*随机数生成	操作系统随机数质量符合 GM/T 0005《随机性检测规范》或 GB/T32915《信息安全技术二元序列随机性检测方法》
146.	安全要求		*内置数字证书	操作系统内置国家电子认证根 CA 的根证书
147.	安全要求		*密码协议实现	操作系统支持符合 GB/T 38636—2020 的 TLCP
148.	安全要求	*安全管理	*防火墙	操作系统提供防火墙配置管理工具，支持基于协议、网络地址、端口的访问控制规则配置，规则修改后立即生效；支持关闭指定服务和端口，包括但不限于关闭远程访问、共享访问等；支持防止 ARP 欺骗攻击
149.	安全要求		*安全框架	操作系统提供统一访问控制安全框架
150.	安全要求	*身份鉴别	*身份鉴别服务	用户标识使用帐户名和帐户 ID，在操作系统的整个生存周期内用户标识具有唯一性；支持用户口令复杂度校验及强口令管理；支持用户口令有效期配置；支持口令鉴别失败控

				制；支持口令加密算法配置，用户口令进行加密后以不可逆的密文形式保存；支持禁止根帐户（root）远程登录设置
151.	安全要求	*访问控制	*自主访问控制	允许客体拥有者以普通帐户决定并控制对客体的访问，并阻止非授权用户对客体的访问；普通用户缺省拥有新建、读写和删除私有目录下文件的权限；支持细粒度的自主访问控制，将访问控制的粒度控制在单个用户，对系统中的每一个客体，实现由客体拥有者以指定用户方式确定其对该客体的访问权限，而其他同组用户或非同组的用户和用户组对该客体的访问权则由客体拥有者授予
152.	安全要求		*强制访问控制	操作系统支持对应用程序的访问控制与资源限制，包括对文件、网络等客体的访问控制；支持应用安装控制、应用执行控制
153.	安全要求		*安全审计	操作系统能对身份鉴别的使用、自主访问控制、标记和强制访问控制策略的修改等生成审计日志；审计记录包括：事件类型、事件发生的日期、触发事件的用户、事件成功或失败等字段；支持审计日志查询和导出功能
154.	安全要求	*漏洞管理	*漏洞管理	操作系统支持漏洞编号，每个漏洞独立编号，可直接使用 NVDB、CNVD 或 CVE 编号；漏洞提醒，发现或获悉漏洞信息时，通过系统推送、电子邮件或官方网站等方式通知用户；漏洞修复，对已发现的安全漏洞通过补丁等方式对系统漏洞进行修复；漏洞列表，提供每个版本已修复的漏洞列表，提供命令或网页等方式方便用户查询漏洞及其修复情况