

项目需求

1. 项目概述

1.1. 项目背景及目标

自 2018 年，上海化学工业区大数据云计算中心一期系统启动建设，系统建成后，已形成一个成熟、安全的硬件资源池，为各部门提供各类网站托管、数据存储、大型计算、系统应用推广、软件开发测试等云资源服务。系统实现了跨部门的数据交换，形成了内部的信息资源共享交换平台，满足了第一阶段安全可靠运行的需要。

上海化学工业区大数据云采用云计算技术，统筹利用已有的 IT 资源和条件，统一建设并为上海化工区管委会各部门及驻区管理单位提供基础设施、支撑软件、应用功能、信息资源、运行保障和信息安全等服务。

1.2. 采购服务内容及应用范围

本次拟启动的云资源服务采购工作，在合同生效之日后 30 日内，完成本项目约定云资源服务提供，并于交付验收通过之日起 12 个月内按照本项目要求提供服务；服务对象涵盖化工区云服务（一期）、化工区云扩容（二期）、驻区管理单位信息系统购买云服务项目、化工区信创云服务项目支撑的机关各处室及驻区单位的 36 个业务系统，共计 276 台主机；服务内容包括：基础设施服务、安全服务、网络链路服务。

2. 总体需求

2.1. 资源需求

经调研各单位、各部门所需计算、存储、网络资源等 IT 基础设施和服务能力需求如下：

序号	项目名称	参数指标	单位	需求数量
----	------	------	----	------

1	云主机	CPU	核	554
		CPU(XC)	核	978
		内存	GB	1578
		内存 (XC)	GB	3844
2	云存储	应用存储空间	TB	129.3
		数据备份服务	TB	129.3
3	云网络	互联网公有 IP 服务	个	34
		互联网带宽 (骨干级)	GB	2
		应用负载均衡服务	每 IP	16
		安全交换区 (网闸)	每 IP	283
4	云安全	网络访问控制服务	租户	63
		入侵防御服务	租户	63
		用户管理服务	租户	63
		用户身份认证服务	租户	63
		VPN 接入	隧道数	63
		在线防护 WAF	套	54
5	云增值服务	基础设施服务：技术支持服务、数据中心运维服务、业务系统运维服务等	套	1
6	链路服务	上云相关链路	条	10
7	密码服务	安全认证网关服务	套	9
		签名验签服务	套	10

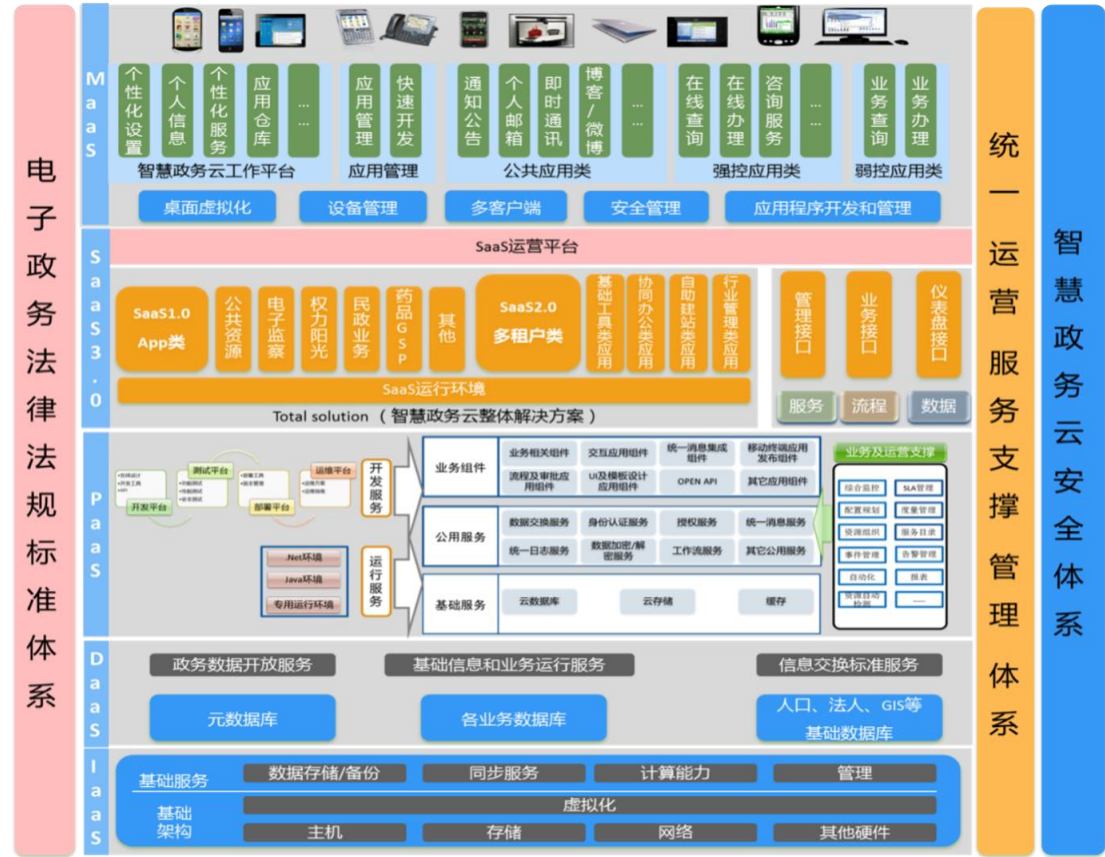
		可信密码服务	应用	9
8	等保服务	等保三级服务	套	1

2.2. 工期要求

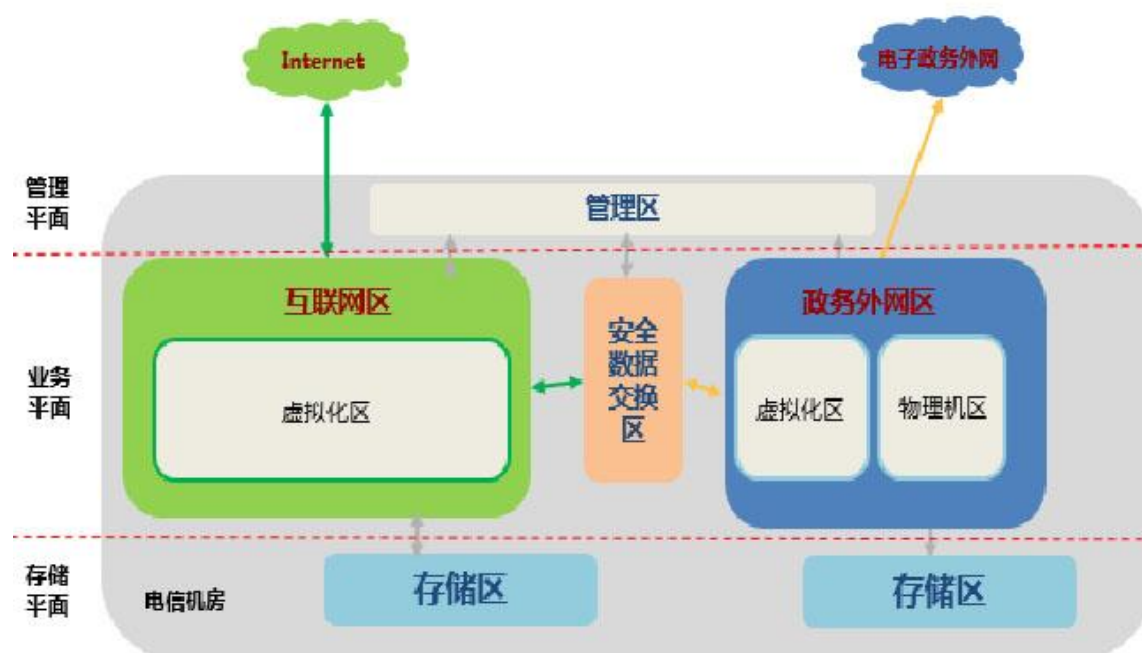
合同生效之日后 30 日内完成本项目约定云资源服务提供。

2.3. 总体架构

上海化工区的设计本着统一规范、成熟稳定、适度超前、开放适用、安全可靠的原则，按照“1+6+X”的应用建设体系进行规划，按照低成本、轻资产、部署快、T3 以上等级的要求，提供云计算服务，以及采用先进的虚拟云数据中心技术，将园区信息服务管理方式由当前“块状”管理调整为基于云数据服务平台的集中管理，建设统一承载和管理园区的“1+6+X”应用体系的基础平台，满足上海化工区多领域资源需求。



系统架构示意图



总体部署架构图

云中心内部署架构主要包括政务外网接入区、政务网云核心交换区、政务外网云资源区、政务外网备份区、政务外网存储区、公共云管理区、安全数据交换区、互联网接入区、互联网云核心交换区、互联网云资源区。

2.4. 项目团队要求

项目经理职责：项目经理应受公司总经理任命和委托，全权负责项目运维的各项工作。需对运维项目的优质、高效、安全负全责。

驻点工程师职责：负责对小型机、服务器、存储设备相关的申报事件进行处理和解决；负责对小型机、服务器、存储设备提供日常性能和运行状况监控，对故障进行分析处理及建立完善预警机制；负责保障机房服务器正常运行，遵循用户的安全保障管理要求；接受用户对服务器维护事件的督办、检查，协助服务台完成对用户意见进行回访和事件统计、分析。对服务过程和反馈的意见进行改进，同时接受服务台的绩效考评工作；及时提供服务器运行和问题处理情况，并向用户负责，并按周、月、季、年提交运维服务工作进度总结和计划；负责整理和归纳服务器日常维护知识库，提交至运维服务平台；负责整理和提交服务器运维过程资料和相关配套维护文档。

技术支持专家职责：为客户提供 7×24 小时的故障响应电话支持；接听客户服务热线

电话和接收（电话/Email/Fax 等）客户服务请求；通过网络或电话为客户提供即时的远程技术支持，包括软硬件故障的诊断和排除，客户端软件的安装和设置；协调多方服务团队，及时跟进未完成的服务请求并及时更新系统信息和状态。

备品备件管理员职责：组织实施备品备件的订购、运输及入库工作；负责汇总待料备件，及时采购或调拨，并主动向项目经理说明待料原因、追踪处理。

2.5. 培训要求

投标人需对本项目的管理及维护人员、系统用户进行培训。

项目管理培训：投标人需对重要岗位的项目管理人员进行专业化的项目管理培训并进行必要的资格认证，对一般管理人员进行有关知识普及性培训，从总体上提高项目管理人员对有关工程项目的管理水平。

系统建设与日常维护培训：投标人应以集中的形式，注重理论与实践相结合，聘请相关领域专家对技术人员和系统维护人员进行专题研讨和技术培训，以确保建成后的系统能稳定运行。针对技术管理及维护人员，除需要针对应用系统的使用、技术架构、常见故障排除等内容进行培训外，还应重点进行数据库、中间件等支撑软件平台的运行维护培训。该类培训必需按照系统管理员级别进行特殊培训，务必使技术人员掌握系统所提供的各项管理维护工具，并尽量了解一些底层调试及操作知识。此外，所有系统维护人员均必需强制接受信息安全培训，熟悉安全管理方针、制度及预案。

3. 具体技术及服务要求

3.1. 服务总体要求

为了完善按需应变的计算环境，建设既要考虑技术先进性，又要遵循简化、共享、标准、动态的原则进行：

标准化：本项目提供的云平台应符合国家和市有关云平台的技术标准和规范要求，包括但不限于国家工信部《基于云计算的电子政务公共平台顶层设计指南》《信息安全技术云计算服务安全指南》（GB/T31167-2014）、《信息安全技术云计算服务安全能力要求》（GB/T31168-2014）、《关于加强党政部门云计算服务网络安全管理的意见》（中网办发〔2014〕14号）。

开放性：本项目提供的云平台在体系结构、设备选型、数据交换等方面应可兼容各种主流的应用系统环境。提供开放的技术接口，满足采购人基于云平台进行部分软件系统二次开发的要求。

先进性和成熟性：本项目提供的云平台应采用先进且成熟可靠的技术，优先选择国内具有自主知识产权且已有成熟案例的软硬件产品，确保在相当长的时期内保持业务系统的可维护性和可扩展性。

安全性：本项目提供的云平台整体技术架构、数据访问机制、数据存储与更新机制、权限管理与控制机制等，必需符合系统安全性的要求。

易用性：本项目提供的云平台应操作简单、使用方便，且易于管理和维护。

可移植性：本项目提供的云平台的接口应保证采购人的业务系统及其数据迁移的兼容性。

业务可用性：本项目提供的云平台整体可用性应不低于 99.9%，数据可靠性应不低于 99.9999%。

3.2. 机房要求

本期项目的投标人为招标方提供的机房应当具备环保措施、消防措施、安全和卫生措施以及节能措施。考虑化工区高危特性（以及未来化工工业互联网的演进，对网络的时延以及带宽具有很高的要求）。因此，云资源需要就近部署，云机房应在化工区范围内为佳。

指标项	规格或技术要求
建设标准	（1）满足 GB50174-2008《电子信息系统机房设计规范》中的 B 级机房建设标准的要求。
	（2）机房的全年服务可用性≥99.99%
机房地点与空间布局要求	（1）提供的机房应在奉贤区范围内，机房在化工区内为佳。
	（2）机房为投标人自有资产为佳（需出具产证证明文件）。
	（3）投标人为本项目提供的机房空间面积初期可容纳≥30 个 42U16A 机柜，并具备平滑扩容至 60 个机柜的空间的能力。
	（4）投标人为本项目提供的机房空间，除满足本项目所有设备运行的需求之外，如采购人需要，还需提供本项目之外的其他设备的机房托管服务。

	(5) 提供与机房在同一大楼内不小于 15 平方米的办公场地，供采购人使用，用于测试、应用部署及业务系统迁移等工作。
动力保障	(1) 电气系统由双路独立市电供应，不小于 500kVA。此外配置柴油发电机作为后备电源，可在满载情况下持续运行 8 小时以上。每套设备机架由两套不同 UPS 供电，每套 UPS 系统均配备独立的电池组，电池组能提供 30 分钟的不间断供电。机房配备油机，满足冗余备份，支持自动启停。
	(2) 每机柜提供双路不间断供电，电力总功率：低密度区每机柜不低于 3KW，高密度区每机柜不低于 5KW。
空调系统	(1) 机房运行环境恒温恒湿：温度为 21--25℃，相对湿度保持在 40%~70%。
	(2) 机房内机柜采用精确送风方式。
	(3) 机房空调系统采取 N+1 冗余备份方式设置，无单点故障。
	(4) 有专业空调维护队伍；对机房温湿度有监控措施和记录。
消防系统	(1) 具备火灾报警及消防联动控制系统。
	(2) 采用七氟丙烷气体消防措施。
	(3) 机房内配备手动或自动气体灭火设备。
	(4) 配置烟雾报警系统，及时侦测火灾隐患，赢得处理时间，降低火灾危害。
机房安防	(1) 7*24 小时保安值班，严格的安全检查与身份认证。
	(2) 各机房出入口及周边均配置门禁及视频监控系统。
	(3) 本项目机房及相关区域的监控录像至少保存 3 个月。必要时，采购人有权查看相关监控录像。
抗震烈度	(1) 机房抗震烈度应达到 8 级或以上。
运维保障	(1) 提供 7*24 小时的值班监控以及应急响应服务。
	(2) 具备电信级智能网络运行监控平台，实时监控机房运行状态，采购人有权远程查看相关信息。
	(3) 由投标人负责机房运行环境的运维保障，包括但不限于机房门禁管理、安防管理、人员出入管理、设备出入管理；机房定期

	环境清洁、物品整理、机房环境监测（温湿度、摄像头、空调等）、机房环境整改；机房消防设施管理、日常消防检查；防雷、防强电管理，地线、电阻管理；电力系统维护、UPS 管理、电机设备管理；应急预案制定及应急演练等。
	（4）采购人或其授权人员有权随时进入投标人机房对本项目所配备的资源进行现场操作，投标人应提供配合与技术支持。

3.3. 计算资源池设计要求

上海化学工业区公共事务中心补充购买服务资源量的要求如下：

序号	项目名称	参数指标	单位	需求数量
1	云主机	CPU	核	554
		CPU(XC)	核	978
		内存	GB	1578
		内存（XC）	GB	3844

3.3.1. 计算资源池总体架构

根据上海化工区电子政务外网云平台的总体架构以及网络架构设计中对功能区的划分原则，将服务器等关键设备按照需要实现的功能划分为两个层面，分别对应业务层和计算平台层。

业务层中，功能区域的划分一般都是根据安全和管理需求进行划分，各个政务部门可能有所不同，总的原则是在满足安全的前提下尽量统一管理。

本期项目投标人建设的计算资源区应提供虚拟化资源池和物理服务器资源池。虚拟化资源池用于部署大部分的政务业务系统，物理资源池用于部署数据库等高负载系统。管理、安全区需规划管理资源池用于部署云管理系统。

3.3.2. 虚拟计算资源池设计要求

对于不同业务的服务器需求，首先需要判断该业务服务器是否能够采用虚拟化方案，不能虚拟化的则应采用满足实际需求的服务器进行配置，能虚拟化部署的业务则应统一采用虚拟化方式部署。

虚拟化集群配置

X86 集群单节点配置 2 颗 32 核/64 线程处理器、1TB DDR4 内存及 2 块 3.84TB NVMe SSD；信创集群单节点配置 2 颗国产化 32 核处理器（32 核）、512GB DDR4 内存及 2 块 1.92TB SATA SSD。虚拟化资源分配遵循 CPU 超分比 $\leq 3:1$ 、内存超分比 $\leq 1.5:1$ ，存储性能需保障随机读写 IOPS 不低于 5000。

物理资源池

数据库服务器采用 4 路 64 核/128 线程处理器、2TB 内存，配置 HBA 卡及 RDMA 高速网卡；存储节点采用 36 盘位全闪存架构，支持 NVMe-oF 协议，数据访问时延 $\leq 200\mu s$ 。

3.3.3. 物理计算资源池设计要求

下列条件下，应直接使用物理机来满足业务对计算资源的需要：

1. 对服务器运算性能要求特别高，在单个物理服务器上配置最大计算能力的虚拟机依然不能满足业务应用的计算能力要求；
2. 现有软件许可加密方式不支持虚拟化的场景；
3. 业务应用对服务器有特别板卡要求且板卡不支持在虚拟化环境中运行。

对应用虚拟化的适应性也可以采用当前主流的应用分层（Web 服务器、App 服务器、DB 服务器）来进行考虑，通常情况下虚拟化比较适合 Web 服务器和 App 服务器。DB 服务器需要根据业务应用对存储 I/O 的需求来评估，如果业务应用的 DB 服务器 I/O 要求大或 DB 服务器有 HA 或集群需要，则建议将该种业务应用的 DB 服务器部署在物理服务器上。

3.3.4. 集群规划设计要求

本期项目投标人提供的虚拟化应基于虚拟化软件，具备基础的虚拟化功能，提供服务

器、存储、网络的虚拟化功能，并向上对 OpenStack 提供接口。一个物理集群中可以把多台服务器划分成一个资源集群，支持虚拟机热迁移和 HA 功能，一个计算资源池应使用相同的调度策略。计算资源池不包括网络资源与存储资源。一个物理集群中可以包含多个资源集群。

分区下的虚拟化服务器配置为若干个虚拟化集群，可实现集群内的资源高可用。而分区的物理机资源将配置在一个大的逻辑服务器集群内。由于本期虚拟化服务器配置与一期新建项目服务器配置不同，投标人应增加分区进行管理。

通过在服务器上部署虚拟化软件将硬件资源虚拟化，从而使一台物理服务器可以承担多台服务器的工作。通过 IT 系统基础设施逐步云化部署，基于云平台虚拟化技术实现计算资源的虚拟化、资源共享、灵活分配，实现业务服务器的整合和调配，集中化以及基于策略的管理，以适应快速发展的业务需求，降低 IT 总持有成本，聚焦核心业务发展。

3.4. 存储资源池设计要求

序号	项目名称	参数指标	单位	需求数量
1	云存储	应用存储空间	TB	129.3
		数据备份服务	TB	129.3

本次项目投标人应提供的存储资源包括：应用存储空间 129.3TB（可用空间）、数据备份服务 129.3TB。投标方需承诺按招标方的 RAID 配置实际使用要求进行部署。

3.4.1. 存储资源池设计总体架构

本期项目投标人为采购方部署的存储资源池应当提供 SAN（并支持 FC SAN 及 IP SAN 传输方式）、NAS 等存储方式，并具备存储虚拟化功能。

3.4.2. 存储资源池设计要求

上海化学工业区存储资源池使用一套 FC/IP-SAN 高端集中存储支撑化工区云计算中心，配置 2 台 FC-SAN 和 2 台 IP-SAN 交换机，存储设备选型为融合存储，同时支持 SAN、NAS 存储，SAN 存储支持 FC-SAN、IP-SAN 组网；存储网络选型为 FC-SAN、IP-SAN、NAS，分别用于高性能计算节点、虚拟化资源池存储、非结构化数据存储。

本次项目投标人应提供的计算资源包括：应用存储空间 129.3TB（可用空间）、数据备份服务 129.3TB。投标方需承诺按招标方的 RAID 配置实际使用要求进行部署。

3.4.3. RAID 配置要求

关于 RAID 的配置，投标人应当依照以下要求：

- 1. 针对典型业务应用，综合考虑性价比，应使用 RAID5；
- 2. 针对数据库等大量存储 I/O 应用，应使用 RAID10；
- 3. 如果磁盘类型选择 SATA/NL-SAS 硬盘，由于硬盘容量大，考虑到数据可靠性，应使用 RAID6。

按照以上原则，可以根据不同性能类型的硬盘，创建具有多层 Raid 策略的融合存储池。同时可以根据不同业务的实际 I/O 使用情况，进行动态磁盘的性能调整。使整体存储池能够兼具高效性、灵活性、先进性。

3.5. 云网络资源池设计

3.5.1. 网络资源要求

本次项目投标人应当为招标方提供的网络资源能力如下：

序号	项目名称	参数指标	单位	需求数量
1	云网络	互联网公有 IP 服务	个	34
		互联网带宽（骨干级）	GB	2
		应用负载均衡服务	每 IP	16
		安全交换区（网闸）	每 IP	283

3.5.2. 网络建设要求

根据上海化工区大数据云平台整体的规划目标以及一期系统建设成果，投标人提供的云数据中心网络架构应满足以下要求：

- 1.高效性：为了满足云平台、电子政务的业务应用系统的高并发、快速的虚拟机迁移

和大文件的上传下载等要求。因此设计一个高带宽、低延时、快速收敛并避免环路出现的网络平台是一个基本的设计目标。

2.高可靠性：云数据中心今后要支持上海化工区电子政务的业务系统，云数据中心的网络的稳定性直接关系到化工区电子政务服务的可用性。因此高可用性是数据中心网络平台的设计目标之一，关键和核心部分不能出现单点故障。

3.可扩展性：随着后续越来越多的业务应用系统迁入云数据中心，云数据中心的规模需要根据业务应用需求逐步扩大。因此具备良好的扩展能力也是数据中心网络平台的设计目标之一，在核心、骨干网络设备上要留有余量，充分考虑今后业务应用增加的网络需求。

4.灵活性、易维护性：云数据中心今后所承载的各个行业电子政务业务系统的不确定性，这就要求网络平台能够灵活简便地对网络资源进行调配。因此，网络管理的灵活性和易维护性也是网络平台的设计目标之一。通过减少网络配置节点、简化网络配置，降低网络管理的人力开销，从而易于网络资源的调整和分配。

5.先进性：云数据中心承载各个下属单位不同种类的电子政务应用系统，整体架构应当保持稳定而不应当频繁调整。作为云数据中心的重要组成部分，网络平台的架构调整会影响云数据中心的整体架构。因此在设计网络平台架构的时候，设计目标之一应该是保证网络架构和采用技术的先进性，3年内只做规模扩充，而不做架构调整。

6.安全性：网络安全是云数据中心安全架构的一个重要组成部分，因此安全性也是网络平台需要考虑的设计目标之一。由于网络安全域的划分与隔离很大程度上依赖网络结构的合理性，因此在设计网络架构的时候需要考虑整体网络安全性，便于安全方案进行安全域的划分和安全域间访问控制。

7.延续性：提供应用迁移涉及线路的IP地址数量满足招标要求，确保化工区各上云单位的IP地址不变，不影响采购人业务连续性。

3.5.3. 网络总体架构设计要求

云中心内部署架构主要包括政务外网接入区、政务网云核心交换区、政务外网云资源区、政务外网备份区、政务外网存储区、公共云管理区、安全数据交换区、互联网接入区、互联网云核心交换区、互联网云资源区。依据项目目标、需求分析和云数据中心的总体架构，网络平台的架构设计应当满足如下条件：使用网络虚拟化和二层结构技术、具备三个独立的网络平面、根据业务功能分区。

网络性能指标

业务平面：采用 100G Spine-Leaf 架构与 CLOS 组网，跨机架传输时延 $\leq 10\mu s$ ，可靠性 $\geq 99.999\%$ 。

存储平面：同时部署 32G FC 与 100G RoCEv2 双平面，时延 $\leq 50\mu s$ ，可靠性 $\geq 99.99\%$ 。

管理平面：独立 10G 带外网络，实施 ACL 白名单管控机制。

安全隔离方案

基于 VXLAN 实现业务系统级逻辑隔离，支持虚拟机级微分段控制。

东西向流量防护采用分布式虚拟防火墙，策略执行时延 $\leq 5ms$ 。

部署网络流量探针（NPB）实现全流量威胁分析，支持异常行为实时告警。

3.5.4. 网络功能区设计要求

为了满足业务系统对网络功能要求，应在数据中心专门部署网络服务区，针对性为各种业务系统提供相应的网络服务。网络服务区应当主要提供 2 种网络服务：一种是网络安全服务，通过部署防火墙设备实现；另外一种应用负载均衡服务，为业务系统增强扩展性、可靠性和业务处理能力，该服务通过部署应用负载均衡设备 LB 实现。

本期项目投标人为招标方建设的上海化学工业区公共事务中心网络架构应满足以下要求：

1. 高效性：采用网络虚拟化及二层网络结构，在提供快速网络带宽的同时，大大降低网络复杂度，网络路径快速收敛，避免网络环路而带来的各种问题。同时通过减少交换层数量，流量需要穿越的交换机数量也会减少，从而可以缩短延迟，提高应用性能。

2. 高可靠性：网络节点采用 CSS、iStack 等集群部署方案，可有效保障网络节点的高可靠性，同时网络采用冗余链路，可以保障任何一个网络节点或网络线路出现故障时，不会对整个系统和业务产生影响，提高整个网络架构的健壮度。通过交换机虚拟集群和堆叠技术，可以消除网络中的可靠性隐患，无需运行 spanning-tree 协议，消除网络的故障收敛时间，从而提高网络可靠性。网络业务区域层次分明，不同区域或者业务访问适配不同基础安全属性，最大程度保障云数据中心资源以及用户业务的网络安全

3.可扩展性：采用可堆叠、可集群的扩展性高的网络设备，可随着后续越来越多的业务应用系统迁入云数据中心实现良好的网络扩展性。网络未来演进能力预置，有效支撑大带宽平滑扩容以及 SDN 和 VXLAN 云网络技术平滑部署，最大程度保证网络具备持续的先进性

4.灵活性、易维护性：采用大二层网络设计，能够更有效地适应云计算对于计算资源池和存储资源池的按需调配，更灵活支撑云计算的动态需求。同时大二层网络有效减少网络中的交换机和链路数量，从而降低前期购置成本和后期维护成本。网络多样化的接入方案，提供政府客户二层、三层接入方式，最大限度满足不同业务单位接入政务云业务需求

5.先进性：采用大二层网络结构设计，可以有效支持云计算东西向网络流量的需求，以及未来多数据中心二层打通、虚拟机迁移等需求，保证云平台网络的先进性。

6.安全性：通过网络分区方式，借助防火墙、VLAN、数据交换等隔离方式，将业务系统隔离在不同的网络区域内，实现业务访问的网络控制，提高系统的安全性。同时，每个计算节点配置业务、管理、存储等多套独立的网络链路，降低多个网络平面之间的干扰，提高网络的安全性和稳定性。

3.6. 云安全设计

服务商所提供的云资源，需承载在满足等保三级要求的云平台上，高分通过为佳。

本次项目投标人应为上海化学工业区公共事务中心提供的云安全资源能力如下：

序号	项目名称	参数指标	单位	需求数量
1	云安全	网络访问控制服务	租户	63
		入侵防御服务	租户	63
		用户管理服务	租户	63
		用户身份认证服务	租户	63
		VPN 接入	隧道数	63
		在线防护 WAF	套	54

3.6.1. 云平台安全方案要求

云服务平台统一为所承载的应用提供全面的网络与信息安全服务，采用安全虚拟化等技术逐步构建统一、集中的安全服务能力资源池，安全服务资源池应具备灵活的弹性扩展能力。各应用只需要考虑业务应用的需求建设，不需要再考虑建立独立的安全防护措施，能够大大提高信息系统应用的建设效率，降低系统建设成本。

安全能力资源池应具备包括防火墙、IPS、Web 应用安全防护等功能。

云服务平台应能确保物理设施安全、边界安全防护、主机安全、虚拟化安全、应用安全、认证安全、数据安全、安全管理、上云系统安全等。

基础设施：通过等保三级与商用密码应用安全性评估，安全设备国产化率 $\geq 90\%$ 。

数据安全：全量数据加密采用 BYOK（自带密钥）模式，密钥轮换周期 ≤ 90 天。

容灾体系：构建同城双活（RPO=0，RTO ≤ 5 分钟）与异地灾备（RPO ≤ 15 分钟）多级架构。

安全服务：提供基于 STIX/TAXII 协议的威胁情报订阅，APT 攻击防护响应时间 ≤ 30 分钟。

3.7. 云增值服务设计

本次项目投标人应为上海化学工业区公共事务中心提供的云增值服务如下：

序号	项目名称	参数指标	单位	需求数量
1	云增值服务	基础设施服务：技术支持服务、数据中心运维服务、业务系统运维服务等	套	1

3.8. 备份和容灾服务设计要求

3.8.1. 云主机备份服务设计

云主机的数据快照恢复服务应当可以让用户可自行选择按时间点、按磁盘来进行数据回滚，并不限制数据恢复的次数。同时，快照恢复服务可针对整个主机包括系统及所有磁盘进行快照操作，消除了数据恢复可能产生的“死角”。

3.8.2. 数据级容灾服务设计

需部署云端数据级灾备系统平台，该平台应当可以通过无缝融合云平台的资源，实现当前整个资源共享，成本低廉、部署迅速、灵活弹性的远程灾备服务，在对数据安全性进行严格管理的同时，实现对数据、应用提供最高可用性保证。

3.9. 云管理平台设计

本次项目投标人应为上海化工区提供的云运维服务，包括但不限于原厂驻场工程师服务、云管理平台综合运维服务、协助应用迁移服务等。

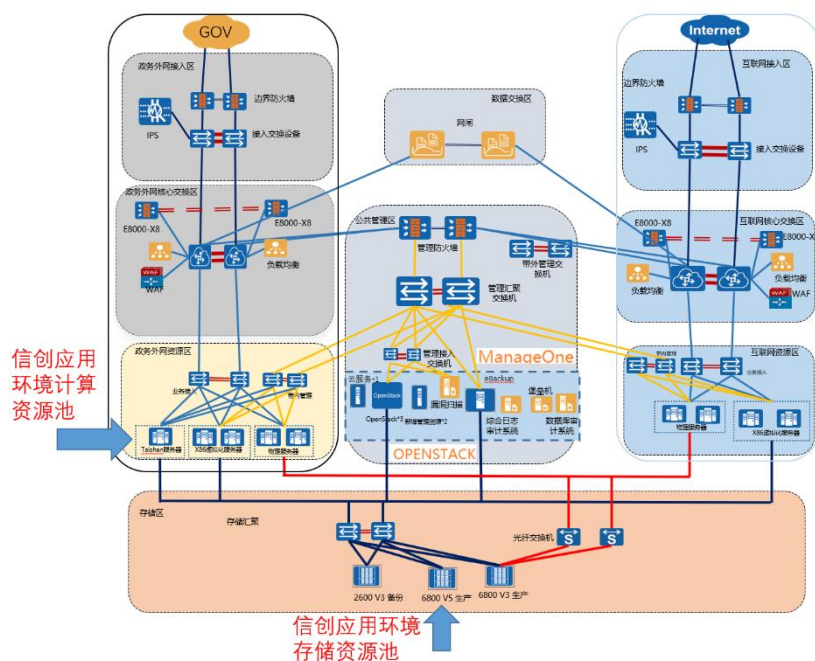
3.9.1. 虚拟化方案设计

本期项目的投标人为招标方设计的虚拟化方案应当具备虚拟化安全隔离、虚拟化热迁移、虚拟化高可用 HA、存储热迁移、虚拟机规格动态调整等功能。

3.9.2. 国产化要求

为满足云平台同时纳管 X86 服务器资源和 ARM 服务器资源，云平台需可以同时支持 X86 和 ARM 架构服务器的计算资源管理。X86 与 ARM 资源池为不同 AZ，相互独立，有效隔离不会互相影响。并需在 ARM 的业务区制作可用于 ARM 服务器的镜像。为保证 ARM 业务系统与原 X86 业务系统的交互和使用效果，X86 与 ARM 资源池必需同机房部署。

相关方案拓扑见下图。



3.10. 密码服务要求

本次项目投标人应为上海化学工业区公共事务中心提供的密码服务如下：

序号	项目名称	参数指标	单位	需求数量
1	密码服务	安全认证网关服务	套	9
		签名验签服务	套	10
		可信密码服务	应用	9

3.10.1. 功能要求

密码服务支撑

提供云平台级密码服务，支持 SM2/SM3/SM4/SM9 等国密算法，覆盖数据加密、数字签名、身份认证等功能。

为租户业务系统提供标准化 API 接口（如 RESTful），支持密钥生成、加解密、摘要计算等基础密码操作。

密钥管理

支持多租户密钥隔离，确保不同租户/应用的密钥独立存储、互不可见。

提供密钥全生命周期管理功能，包括生成、存储、分发、更新、销毁等，密钥需优先存储于硬件密码机（HSM）或合规密钥管理系统。

密码资源管理

实时监控密码服务资源（如密码机性能、API 调用量），动态分配资源以应对业务高峰。

提供可视化监控界面，展示密码服务运行状态、密钥使用统计及告警信息。

3.10.2. 技术要求

合规性要求

遵循 GB/T 39786-2021《信息系统密码应用基本要求》，通过商用密码应用安全性评估。

密码产品需通过国家保密局认证（如服务器密码机、密钥管理系统）。

安全隔离

采用虚拟密码机（vHSM）技术，为每个租户分配独立虚拟密码资源。

租户密钥存储需加密保护，支持硬件级安全隔离（如 TEE/SE）。

高可用性

密码服务集群支持负载均衡，单节点故障时自动切换，服务可用性 $\geq 99.9\%$ 。

密钥管理系统支持异地备份与快速恢复机制。

3.10.3. 服务要求

部署模式

与云平台深度集成，支持私有化部署或混合云模式，提供密码服务与云原生应用的快速对接方案。

接口标准化

提供标准 SDK 及开发文档，支持 Java/Python/C++ 等主流开发语言调用。

运维支持

7×24 小时运维监控，响应时间≤1 小时（重大安全事件）。

每季度提供密码服务健康检查报告及优化建议。

培训服务

提供密码服务使用培训及密评合规指导，协助通过等保三级和密评测评。

3.11. 等保服务要求

依据《信息安全技术网络安全等级保护基本要求》（GB/T 22239-2019）第三级的要求，对 2026 年上海化工区云资源服务项目进行全面的安全评估，包括但不限于物理安全、网络安全、主机安全、应用安全、数据安全及备份恢复、安全管理等方面。

识别现有系统存在的安全隐患，提出整改建议，并协助完成整改工作，确保系统达到等保三级标准。

提供等保三级评估报告、整改建议方案及整改完成后的复测报告。

3.12. 技术服务团队要求

投标人应为本项目组建专业的技术服务团队，提供 7×24 小时的技术服务；技术服务团队的人员构成应涵盖本项目涉及的各个技术领域，具备云平台服务相关的经验和专业技能。

投标人应指定 2 名专职人员作为技术接口人，负责跟踪云平台服务全过程。在服务期间，技术接口人员变更必需征得甲方同意。

对采购人提出的服务请求，投标人必需在 10 分钟内响应，并安排相应的技术人员提供服务。

在合同签订后至项目建设完成前，项目经理和骨干技术人员应常驻现场；对项目的实施制定实施方案，细化到每个执行步骤，每个步骤应包含实施时间、实施内容、具体操作步骤、实施人、监护人，在实施前必需得到采购方和监理方的书面授权。

项目实施包含调整网管软件系统，真实展现调整后的系统平台，设置阈值、告警等，由投标人负责完成，所有相关费用计入投标报价。如投标人进行了非授权操作，将给予警告并记录，如累计 3 次警告，将提交政府相关采购部门进行不诚信记录。

在项目实施和维护过程中，如造成数据损坏或影响业务正常运行，投标人应承担所有

损失。

服务期内，如采购单位需要，投标人应提供不限次数的针对应用系统的安全加固测试、整改、指导、培训等服务。

投标人在采购单位提出要求后的 3 个工作日内，组建包含系统工程师、数据库工程师、网络工程师和安全工程师的团队，到采购单位指定的地点提供安全加固服务。

投标人应做出无推诿承诺。即无论由于哪一方产生的问题而使系统发生不正常情况时，立即派工程师到现场全力协助，直至系统故障原因找到并解决，系统恢复正常。

4. 验收要求

1.服务根据合同的规定完成后，甲方应及时进行根据合同的规定进行服务验收。乙方应当以书面形式向甲方递交验收通知书，甲方在收到验收通知书后的 10 个工作日内，确定具体日期，由双方按照本合同的规定完成服务验收。甲方有权委托第三方检测机构进行验收，对此乙方应当配合。

2.如果属于乙方原因致使系统未能通过验收，乙方应当排除故障，并自行承担相关费用，同时进行试运行，直至服务完全符合验收标准。

3.如果属于甲方原因致使系统未能通过验收，甲方应在合理时间内排除故障，再次进行验收。如果属于故障之外的原因，除本合同规定的不可抗力外，甲方不愿或未能在规定的时间内完成验收，则由乙方单方面进行验收，并将验收报告提交甲方，即视为验收通过。

4.甲方根据合同的规定对服务验收合格后，甲方收取发票并签署验收意见。

中标人承担本项目总体要求框架内的化工云数据中心、基础软件、服务器设备、网络及安全设备等的软硬件设备建设运维费用，并负责化工云平台整体运维。

5. 其他要求

服务团队人员中，具有正高级职称、信息系统项目管理师证书、注册信息安全专业人员（CISP）证书的优先。