ICS 35.240.99
CCS L 70

T/GDEIIA

团　体　标　准

T/GDEIIA xx—2023

政务行业云资源池“双云多芯”建设技术规范

Technical specifications for the construction of "dual-cloud multi-core" cloud resource pools in the government industry

（征求意见稿）

XXXX – XX – XX 发布　　XXXX – XX – XX 实施

广东省电子信息行业协会　　发布

目　　录

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

本文件由XXX提出。

本文件由广东省电子信息行业协会归口。

本文件起草单位：中国电信股份有限公司广州分公司、中通服中睿科技有限公司、天翼云科技有限公司广东分公司、广州市品高软件股份有限公司。

本文件主要起草人：XX\XX。

本文件为首次发布。

政务行业云资源池“双云多芯”建设技术规范

1 范围

本文件规定了政务行业云资源池双云多芯的总体原则、总体架构及技术规范的要求。
本规范适用于政务行业云资源池双云多芯的建设以及应用。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 32400—2015 信息技术 云计算 概览与词汇
GB/T 32399—2015 信息技术 云计算 参考架构
GB/T 35301—2017 信息技术 云计算 平台即服务（PaaS）参考架构
GB/T 36325—2018 信息技术 云计算 云服务 级别协议基本要求
GB/T 36326—2018 信息技术 云计算 云服务 运营通用要求
GB/T 22239—2019 信息安全技术 网络安全等级保护基本要求
GB/T 35279—2017 信息安全技术 云计算安全参考架构
GB/T 31168—2014 信息安全技术 云计算服务安全能力要求
GB/T 31167—2014 信息安全技术 云计算服务安全指南
GB/T 22240—2020 信息安全技术 网络安全等级保护定级指南
GB/T 22239—2019 信息安全技术 网络安全等级保护基本要求
GB/T 33780—2021 基于云计算的电子政务公共平台技术规范
GB/T 34077—2021 基于云计算的电子政务公共平台管理规范
GB/T 34078—2021 基于云计算的电子政务公共平台总体规范
GB/T 34079—2021 基于云计算的电子政务公共平台服务规范
GB/T 34080—2021 基于云计算的电子政务公共平台安全规范

3 术语和定义

下列术语和定义适用于本文件。

1、云计算 cloud computing

一种通过网络将可伸缩、弹性的共享物理和虚拟资源池以按需自服务的方式供应和管理的模式。

2、云服务 cloud service

通过云计算已定义的接口提供的一种或多种能力。

3、云服务类别 cloud service category

拥有某些相同质量集合的一组云服务。

4、双云多芯 dual-cloud multi-core

基于短期内非国产X86架构的云资源池和国产芯片架构云资源池并存，将多种服务器芯片等硬件封装成标准算力，无论底层是X86与ARM的并存、ARM不同厂商架构间并存、亦或是其它不同芯片架构并存，都能提供一致的云计算服务。

5、基础设施即服务 infrastructure as a service

为云服务客户提供云能力类型中的基础设施能力类型的一种云服务类别。

6、平台即服务 platform as a service

为云服务客户提供云能力类型中的平台能力类型的一种云服务类别。

7、软件即服务 software as a service

为云服务客户提供云能力类型中的应用能力类型的一种云服务类别。

8、租户 tenant

对一组物理和虚拟资源进行共享访问的一个或多个云服务用户。

9、多租户 multitenant

通过对物理或虚拟资源的分配实现多个租户以及他们的计算和数据彼此隔离和不可访问。

10、虚拟化 virtualization

虚拟化是指计算机元件在虚拟的基础上而不是真实的基础上运行。虚拟化技术可以扩大硬件的容量，简化软件的重新配置过程。CPU的虚拟化技术可以单CPU模拟多CPU并行，允许一个平台同时运行多个操作系统，并且应用程序都可以在相互独立的空间内运行而互不影响，从而显著提高计算机的工作效率。

11、负载均衡 load balance

负载均衡建立在现有网络结构之上，它提供了一种廉价有效透明的方法扩展网络设备和服务器的带宽、增加吞吐量、加强网络数据处理能力、提高网络的灵活性和可用性，通过将访问流量自动分发到多台云主机，扩展应用系统对外的服务能力，实现更高水平的应用程序容错性能。

12、应用系统 application system

应用系统是指为了满足用户的业务需求，向用户提供特定应用功能，由硬件设备、通信网络、系统软件和应用软件共同组成的集合。

13、应用 application

应用是由一个或多个应用系统所提供，用于满足企业特定业务需求的一组相关的软件功能。

14、容器 container

容器是包含代码、运行、系统库和配置等所有依赖关系一个标准的软件单元，具有轻量、快速、隔离和可移植等特性，便于实现应用程序从一个计算环境快速可靠地运行到另一个计算环境。

15、服务 service

可用一系列抽象的、独立实现的、要求服务者和提供服务者直接的交互描述，建模的资源的功能方面的能力。

16、微服务 micro services

微服务是指以服务方式实现的不带界面的软件包，具有部署独立、通信轻量的特点，支撑单一业务逻辑的功能实现，通常用于跨专业的数据交互或并发量大的业务逻辑功能实现。

17、服务目录 service catalog

服务目录是记录服务提供者所提供服务的全部种类以及服务目标情况，为选择服务、检索服务提供支撑的列表。

18、中央认证服务 Central Authentication Service

中央认证服务CAS以SAML规范为基础，提供了一种集中式的用户认证方式。它由两个主要组件组成：CAS服务器和CAS客户端。CAS服务器负责认证用户并为他们提供服务票据，作为认证的证明。CAS客户端被集成到网络应用程序或服务中，负责从CAS服务器请求服务票并验证它们。

19、入侵检测系统 Intrusion Detection System

入侵检测系统是一种对网络传输进行即时监视，在发现可疑传输时发出警报或者采取主动反应措施的网络安全设备。它与其他网络安全设备的不同之处便在于，入侵检测系统是一种积极主动的安全防护技术。

20、入侵防御系统　Intrusion Prevention System

入侵防御系统是计算机网络安全设施，是对防病毒软件和防火墙的补充。入侵防御系统是一部能够监视网络或网络设备的网络资料传输行为的计算机网络安全设备，能够及时地中断、调整或隔离一些不正常或是具有伤害性的网络资料传输行为。

21、网络地址转换　Network Address Translation

网络地址转换也叫做网络掩蔽或者IP掩蔽，是一种在IP数据包通过路由器或防火墙时重写来源IP地址或目的IP地址的技术。这种技术被普遍使用在有多台主机但只通过一个公有IP地址访问因特网的私有网络中。

22、单点登录　Single Sign On

单点登录是一种帮助用户快捷访问平台中多个网元或系统的安全通信技术，基于一种安全的通信协议，通过多个系统之间的用户身份信息的交换来实现。使用单点登录系统时，用户只需要登录一次就可以访问多个系统，不需要记忆多个口令密码，从而提高工作效率和系统的安全性。

23、统一安全管理平台解决方案　Authentication, Authorization, Accounting and Audit

融合统一用户账号管理、统一认证管理、统一授权管理和统一安全审计四要素后的解决方案，涵盖单点登录（SSO）等安全功能，能够为用户提供内部或监管部门要求的报表。

4　缩略语

IaaS：基础设施即服务（Infrastructure as a Service）
PaaS：平台即服务（Platform as a Service）
SaaS：软件即服务（Software as a Service）
VPN：虚拟专用网络（Virtual Private Network）
VPC：虚拟私有云（Virtual Private Cloud）
NAT：网络地址转换（Network Address Translation）
ECC：错误检查和纠正（Error Checking and Correcting）
RAID：磁盘阵列（Redundant Arrays of Independent Disks）
TCP：传输控制协议（Transmission Control Protocol）
UDP：用户数据包协议（User Datagram Protocol）
SSL：安全套接层（Secure Socket Layer）
HPA：水平自动扩缩容（Horizontal Pod Autoscaler）
CronHPA：定时水平自动扩缩容（Cron Horizontal Pod Autoscaler）
RABC：基于角色的访问控制（Role-Based Access Control）
CAS：中央认证服务（Central Authentication Service）
SDK：软件开发工具包（Software Development Kit）
LDAP：轻量目录访问协议（Lightweight Directory Access Protocol）
SID：安全标识符（Security Identifiers）
NIC：网络接口卡/网卡（Network Interface Card）
APT：高级长期威胁（Advanced Persistent Threat）
WAF：Web应用防护系统（Web Application Firewall）
ARP：地址解析协议（Address Resolution Protocol）

HTTP：超文本传输协议（Hypertext Transfer Protocol）
SMTP：简单邮件传输协议（Simple Mail Transfer Protocol）
IMAP：因特网信息访问协议（Internet Message Access Protocol）
FTP：文件传输协议（File Transfer Protocol）
NFVM：网络功能虚拟化管理器（Network Functions Virtualization Manager）
SSL：安全套接层（Secure Socket Layer）
ACL：访问控制列表（Access Control Lists）
4A：统一安全管理平台解决方案（Authentication, Authorization, Accounting and Audit）
SSO：单点登录（Single Sign On）

5 总体原则

5.1 高可靠性及可用性

系统的可靠性包括整体可靠性、数据可靠性和单一设备可靠性三个方面。云平台的分布式架构，从整体系统上提高可靠性，降低系统对单设备可靠性的要求。

系统的可用性是通过冗余、高可用集群、应用与底层设备松耦合等特性来体现，从硬件设备冗余、链路冗余、应用容错等方面充分保证整体系统的可用性。

5.2 安全性与易用性

云平台作为政务应用的承载体，应严格按照国家及行业安全标准规范设计建设，遵照各级保密法律法规，采取切实有效的措施，重点保障网络安全、主机安全、虚拟化安全、数据保护，确保系统安全稳定运行。通过提供统一的 4A 与日志管理功能降低平台安全管理门槛与稽核审查难度。

云平台应操作简单、使用方便、可集中管理和易于维护，用户能够方便灵活地使用各应用资源。

5.3 先进性与实用性

鉴于国产化技术能力，合理利用云计算的技术先进性和理念先进性，兼顾近期与长远的利益，既要考虑技术实用性，用成熟技术实现政务行业云平台，又要考虑技术的先进性和可扩展性，确保技术不落后。采用虚拟化、资源动态部署等先进技术与模式，并与业务相结合，确保先进技术与模式应用的有效与适用。

5.4 智能的云网安融合管理能力

云、网、安通常有相对独立的集成规范和管理系统，政务云平台面对较为复杂多样的网络接入需求和更加严格的网络安全管理要求。平台应当配备统一的管理平台，集约云网安各类网元告警、平台性能分析、安全趋势分析、运维计划任务、报表自动生成等智能管理能力，精简运维所需面对的管理系统数量，提升运维效率与质量。

5.5 开放性与可扩展性

充分融入行业生态，实现硬件、软件厂商无关性。资源根据业务应用工作负荷需求进行弹性伸缩，IT 基础架构应与业务系统松耦合，实现系统的灵活扩展。

5.6 自主可控性

按照相关规定及要求，综合对比各类技术路线和各类产品性能，政务云建设采用自主可控技术路线，

通过构建统一的云计算管理平台引入多家服务提供商，打造完善的“数字政府”云平台，为未来发展预留足够空间。

5.7 标准化与可迁移性

云平台自身技术体制、系统架构、数据结构、软硬件选型，以及其建设和服务提供过程必须符合相关国家标准规定。现有应用系统经科学分析、评估，按需逐步迁移至政务行业云平台，一方面使得政务行业云平台能充分利用既有政务应用资源，另一方面迁移和新建的政务应用能够充分利用云平台集约建设的资源以及云模式提供的各类服务。

6 总体框架

6.1 总体架构

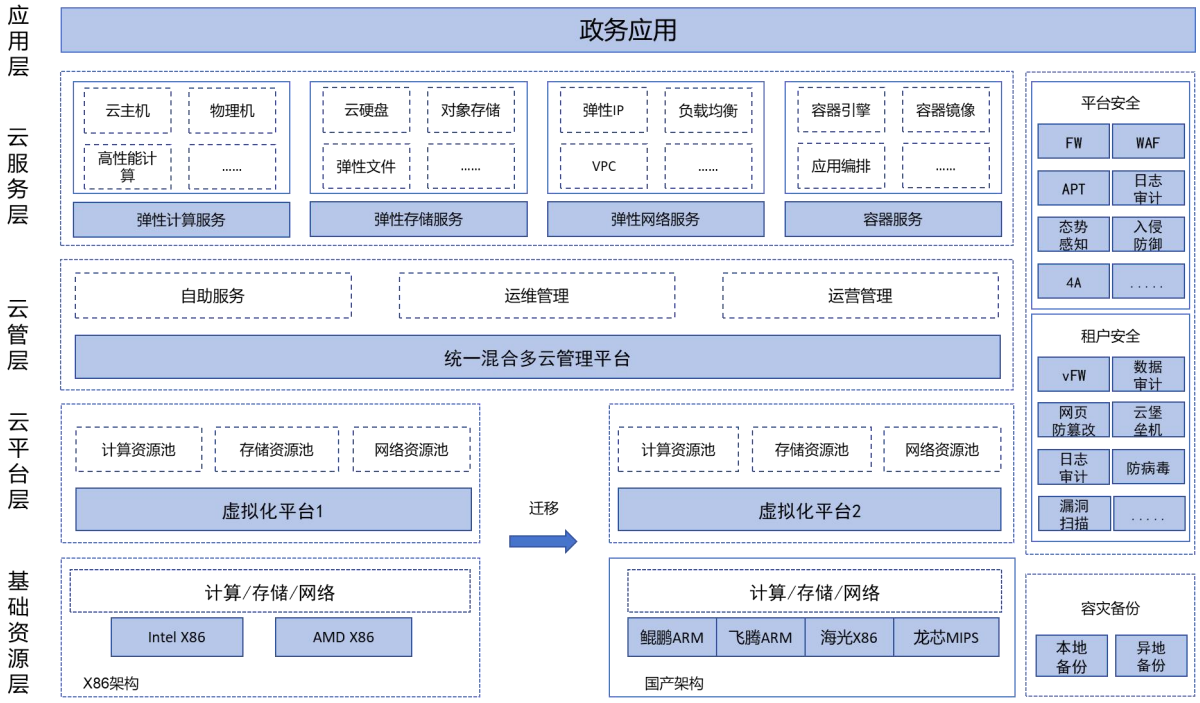

图6-1 “双云多芯”资源池总体架构

“双云多芯”资源池总体架构是基于政务行业云资源池建设所涉及的国家标准、业界主流技术标准、行业标准形成的云平台规范体系，它涵盖了云平台建设所需的基础资源层、云平台层、云管层、云服务层、应用层、云安全体系、云灾备体系等几部分。

6.2 基础资源层

基础资源层是构成“双云多芯”资源池的基础设施，包括计算、存储和网络等硬件设备，用于指导“双云多芯”基础资源的规划、设计与实施，规范基础资源的功能、技术及性能要求，为构建统一的多芯云资源池环境奠定基础。

基于政务云行业资源池现状，一是满足原部署在 X86 架构云资源池的政务应用后续逐步迁移至国产化资源池的需要，二是部署国产化计算/存储/网络等基础设施资源，主要提供鲲鹏 ARM 池、飞腾 ARM 池、海光 X86 池、龙芯 MIPS 池四种计算资源池。

6.3 云平台层

通过国产自研云软件，包括服务器虚拟化、云平台、分布式存储、网络管理等组件，把物理资源转化抽象为池化资源，包括虚拟化计算资源池、虚拟化存储资源池以及虚拟化网络资源池。通过虚拟化云平台对资源池的统一调度和管理，为上层提供丰富的云服务资源。

6.4 云管理平台层

统一混合多云管理平台按照“双云多芯”、异构融合”并行的思路，既支持 ARM 架构的飞腾、鲲鹏芯片，也支持 X86 架构的国产芯片及其他架构芯片，实现异构资源的统一管理和调度，满足应用多样性、稳定性发展的需求。通过资源统一开通、统一运营、统一运维等能力，简化混合云管理，提供包括门户管理、总览管理、服务管理、运营管理、资源管理、运维管理、权限管理、配置管理等功能模块，同时提供 API 接口可用于对接其他管理平台。

6.5 云服务层

云服务层包括弹性计算服务、弹性存储服务、弹性网络服务和容器服务。云服务层通过流程化服务模板和操作向导帮助用户快捷开通云业务。

1、弹性计算服务

弹性计算服务是将计算服务资源化管理，为用户提供统一、集中的云主机、GPU 云主机、物理机、镜像和高性能计算等服务。

2、弹性存储服务

弹性存储服务是将存储资源池化管理，实现存储资源按需交付，提供云硬盘、对象存储、弹性文件、云盘备份和云主机备份等服务，满足用户对弹性化存储服务要求。

3、弹性网络服务

弹性网络服务是面向云计算应用构建的敏捷性资源池化、快速弹性、按需自助的网络服务，包括弹性 IP、负载均衡、VPN 连接、VPC 和 NAT 网关等服务，满足用户各类网络需求。

4、容器服务

容器服务是一种特殊的云计算服务，提供灵活、高效、可扩展的代码容器和应用环境，方便用户在云上快速搭建和管理云端环境，以满足大规模分布式应用系统的需求，具体包括容器引擎、容器镜像、应用编排、微服务引擎和 Serverless 等。

6.6 应用层

应用层主要为在云平台上部署的政务应用。本标准不涉及具体的政务应用及相关软件。

6.7 云安全体系

云安全体系包括云平台安全和租户安全，通过云平台边界安全、宿主机与虚拟化安全及云管理平台安全防护，保障云平台自身安全外，也保障 IaaS、PaaS、SaaS 等主要业务的安全性，并为云租户提供安全能力，在云平台应用国密技术实现对数据的安全加密。

6.8 云灾备体系

要保障政务云的稳定高效运行，除了云安全体系之外还需要一个良好的灾备管理体系，以提供资源、应用的统一的备份、容灾功能。云平台提供数据级容灾服务，备份服务包括本地备份、异地备份服务。

7 技术规范

7.1 基础设施即服务（IaaS）

统一云平台划分成不同类型的资源池，按业务需求灵活申请使用；规划时也按照管理资源池、计算资源池、存储资源池、网络资源池分别规划设计。

- 计算资源池：计算资源池通常映射虚拟化集群；
- 存储资源池：存储资源池通常映射一个共享存储网络；
- 网络资源池：通常映射网元服务器集群和物理网络；

7.1.1 计算资源

7.1.1.1 计算组件部署

计算资源部署独立的计算服务组件，提供高可靠、易扩展的计算服务能力。

国产服务器在国产操作系统的基础上部署虚拟化组件承载虚拟机业务，且同一集群内云主机支持HA 保障业务高可靠。vCPU 可根据业务规划，支持 1:1~1:6 的灵活超配比设置。

计算组件详细部署说明见下表：

表 7-1 计算组件部署说明

节点类型	组件名称	说明
虚拟化节点	国产操作系统	部署在国产服务器之上的宿主机系统
	自研虚拟化组件	自研虚拟化内核，用于承载国产虚拟机业务

7.1.1.2 计算服务器设备选型和参考配置

1、服务器vCPU和内存能力测算

根据典型业务模型进行测算，具体需根据项目实际情况进行调整。单台服务器可提供的 vCPU 能力见下表：

表 7-2 单台服务器 vCPU 能力参考配置

序号	因素	计算公式
C1	单台服务器 CPU 数量	按照服务器实际路数填写
C2	单颗 CPU 物理核数	按照 CPU 规格填写
C3	线程数	鲲鹏:1 / 海光:2 / 飞腾:1
B1	总线程数	B1=C1*C2*C3
C4	系统预留	鲲鹏:6 / 海光:8 / 飞腾:8
K1	DPDK 功能消耗	按照云产品规格中最大收发包（万 pps）实测消耗
C6	总消耗+预留	C4 + K1
B2	实际可用线程数	B2=B1-C6
C7	典型超配比	2
B3	共享型云主机产品可虚 vCPU 数量	B3=B2*C7
B4	独享型云主机产品可虚 vCPU 数量	B2
B5	需要的 vCPU 数量	按实
D1	所需设备台数（共享型）	D1=B5/B3
D2	所需设备台数（独享型）	D2=B5/B4

注：系统消耗线程数为系统运行虚拟化软件等底层系统的必要开销。

单台服务器需配置内存容量见下表：

表 7-3 单台服务器内存容量参考配置

序号	因素	计算公式
A1	需求总内存	按实
C1	根据 vCPU 需求计算的设备台数	见 CPU 测算模型中 D1
A2	单台宿主机需要提供的可用内存	A2=A1/C1
B1	单台宿主机总线程数	见 CPU 测算模型 B1
A3	系统消耗和预留内存	A3=B1*0.75+8
A4	单台宿主机需要配置的总内存数	A4=A2+A3
A5	单条内存容量（G)	按实
S1	实际配置内存条数	S1=A4/A5，向上取偶
A6	实际的内存配置数	A6=A5*S1

注：内存消耗为系统运行虚拟化软件等底层系统的必要开销。

2、服务器可靠性要求

服务器可靠性要求包括内存、硬盘、电源等多个层面的内容。

- 提供 BIOS 内存自检和 ECC 纠错技术；
- 支持硬盘热插拔和 RAID 功能，提供硬盘在线故障检测和预警；
- 支持电源 1+1 冗余和热插拔；
- 支持对 CPU，内存，风扇，电源，硬盘等热关键器件的温度实时监控，设备故障时会产生告警，可以灵活对支持热插拔设备进行在线更换，不支持热插拔设备提前安排好业务后进行下电更换。
- 配合智能的风扇调速和监控，确保系统运行的可靠性。

3、GPU国产化参考配置

表7-4 GPU国产化参考配置

序号	因素	计算公式
C1	单台服务器CPU数量	按照服务器实际路数填写
C2	单颗CPU物理核数	按照CPU规格填写
C3	线程数	鲲鹏:1 / 海光:2
B1	总线程数	B1=C1*C2*C3
C4	系统预留	鲲鹏:6 / 海光:8
K1	DPDK功能消耗	按照云产品规格中最大收发包（万pps）实测消耗
C6	DPDK消耗+系统预留	C4 + K1
B2	实际可用线程数	B2=B1-C6
B4	GPU不超配可虚vCPU数量	B2

4、服务器参考配置要求

（1）计算节点服务器

表 7-5 计算节点服务器 I 参考配置

项目	参考指标
CPU	鲲鹏处理器，主频 2.6GHz，核数 48 核，处理器数量 2 颗
内存	≥384GB DDR4

项目	参考指标
存储	≥2 块 480G SATA SSD 硬盘
网卡	≥4*GE 网口 ≥6*10GE 网口 ≥2*双口 HBA 卡
缓存	≥2GB 缓存，支持缓存数据保护，支持 RAID 0，1，5，6

表 7-6 计算节点服务器 II 参考配置

项目	参考指标
CPU	鲲鹏处理器，主频 2.6GHz，核数 32 核，处理器数量 2 颗
内存	≥256GB DDR4
存储	≥2 块 480G SATA SSD 硬盘
网卡	≥4*GE 网口 ≥6*10GE 网口 ≥2*双口 HBA 卡
缓存	≥2GB 缓存，支持缓存数据保护，支持 RAID 0，1，5，6

表 7-7 计算节点服务器III参考配置

项目	参考指标
CPU	飞腾处理器，主频 2.1GHz，核数 64 核，处理器数量 2 颗
内存	≥512GB DDR4
存储	≥2 块 480G SATA SSD 硬盘
网卡	≥4*GE 网口 ≥6*10GE 网口 ≥2*双口 HBA 卡
缓存	≥2GB 缓存，支持缓存数据保护，支持 RAID 0，1，5，6

表 7-8 计算节点服务器IV参考配置

项目	参考指标
CPU	海光处理器，主频 2.0GHz，核数 32 核，处理器数量 2 颗
内存	≥256GB DDR4
存储	≥2 块 480G SATA SSD 硬盘
网卡	≥4*GE 网口 ≥6*10GE 网口 ≥2*双口 HBA 卡
缓存	≥2GB 缓存，支持缓存数据保护，支持 RAID 0，1，5，6

（2）物理服务器

表 7-9 物理服务器 I 参考配置

项目	参考指标
CPU	鲲鹏处理器，主频 2.6GHz，核数 48 核，处理器数量 2 颗
内存	≥256GB DDR4

存储	≥2 块 480G SATA SSD 硬盘，≥2 块 8T SATA 硬盘
网卡	≥4*GE 网口 ≥6*10GE 网口 ≥2*双口 HBA 卡
缓存	≥2GB 缓存，支持缓存数据保护，支持 RAID 0，1，5，6

表 7-10 物理服务器 II 参考配置

项目	参考指标
CPU	鲲鹏处理器，主频 2.6GHz，核数 32 核，处理器数量 2 颗
内存	≥512GB DDR4
存储	≥2 块 480G SATA SSD 硬盘，≥2 块 8T SATA 硬盘
网卡	≥4*GE 网口 ≥6*10GE 网口 ≥2*双口 HBA 卡
缓存	≥2GB 缓存，支持缓存数据保护，支持 RAID 0，1，5，6

表 7-11 物理服务器III参考配置

项目	参考指标
CPU	飞腾处理器，主频 2.1GHz，核数 64 核，处理器数量 2 颗
内存	≥256GB DDR4
存储	≥2 块 480G SATA SSD 硬盘，≥2 块 8T SATA 硬盘
网卡	≥4*GE 网口 ≥6*10GE 网口 ≥2*双口 HBA 卡
缓存	≥2GB 缓存，支持缓存数据保护，支持 RAID 0，1，5，6

表 7-12 物理服务器IV参考配置

项目	参考指标
CPU	龙芯处理器，主频 1.8GHz，核数 4 核，处理器数量 4 颗
内存	≥128GB DDR4
存储	≥2 块 256G SATA SSD 硬盘，≥2 块 8T SATA 硬盘
网卡	≥4*GE 网口 ≥4*10GE 网口
缓存	≥2GB 缓存，支持缓存数据保护，支持 RAID 0，1，5，6

表 7-13 物理服务器V参考配置

项目	参考指标
CPU	海光处理器，主频 2.5GHz，核数 16 核，处理器数量 2 颗
内存	≥256GB DDR4
存储	≥2 块 480G SATA SSD 硬盘，≥2 块 8T SATA 硬盘
网卡	≥4*GE 网口

项目	参考指标
	≥6*10GE 网口 ≥2*双口 HBA 卡
缓存	≥2GB 缓存，支持缓存数据保护，支持 RAID 0，1，5，6

7.1.2 存储资源

7.1.2.1 存储组件部署

云资源池存储组件部署的分布式块存储资源池，能独立提供高可用、高可靠且易扩展的分布式存储能力。存储组件见下表：

表 7-14 存储组件

节点类型	组件名称	说明
块存储节点	engine	分布式存储软件，根据配置的冗余模式，将数据分片打散的分布到多个故障域的存储节点
	disk-cache	分布式存储缓存软件，用作数据缓存使用，分散部署在所有服务器上
监控服务	monitor	存储管控平台的监控软件部署，主备模式部署，虚机部署

7.1.2.2 存储服务器选型和参考配置

根据典型业务模型进行测算，具体需根据项目实际情况进行调整。分布式块存储、对象存储、文件存储在不同存储策略下的能力参考配置见下表：

1、HDD分布式块存储

表 7-15 HDD 分布式块存储参考配置

序号	因素	计算公式
A1	存储容量需求（TB）	按实
A2	副本数	3
A3	存储复用比	1
A4	存储使用率水位	85%
A5	格式化损耗（容量换算系数）	11%
S1	裸容量需求（TB）	S1=A1*A2/A3/A4/(1-A5)
B1	每台服务器 HDD 数量	按实
B2	单 HDD 容量（TB）	按实
A6	单台服务器存储（TB）	A6=B1*B2
S2	存储服务器数量（台）	S2=S1/A6（向上取整）

2、SSD分布式块存储

表 7-16 SSD 分布式块存储参考配置

序号	因素	计算公式
A1	存储容量需求（TB）	按实
A2	副本数	3
A3	存储使用率水位	85%
A4	格式化损耗（容量换算系数）	11%

序号	因素	计算公式
S1	裸容量需求（TB）	S1=A1*A2/A3/(1-A4)
B1	每台服务器 SSD 数量	按实际配置填写
B2	单 SSD 容量	按实际配置填写
A5	单台服务器存储（TB）	A5=B1*B2
S2	存储服务器数量（台）	S2=S1/A5（向上取整）

3、对象存储（三副本）

表 7-17 对象存储（三副本）参考配置

序号	因素	计算公式
A1	存储容量需求（TB）	按实
A2	副本数	3
A3	存储使用率水位	85%
A4	格式化损耗（容量换算系数）	11%
S1	裸容量需求	S1=A1/A2/A3/(1-A4)
B1	每台服务器 HDD 数量	按实
B2	单 HDD 容量	按实
A5	单台服务器存储（TB）	A5=B1*B2
S2	存储服务器数量（台）	S2=S1/A5（向上取整）（3 台起配）

4、对象存储（纠删码，4+2）

表 7-18 对象存储（纠删码，4+2）参考配置

序号	因素	计算公式
A1	存储容量需求（TB）	按实
A2	EC（4+2）	66%
A3	存储使用率水位	85%
A4	格式化损耗（容量换算系数）	11%
S1	裸容量需求	S1=A1/A2/A3/(1-A4)
B1	每台服务器 HDD 数量	按实
B2	单 HDD 容量	按实
A5	单台服务器存储（TB）	A5=B1*B2
S2	存储服务器数量（台）	S2=S1/A5（向上取整）（6 台起配）

5、对象存储（纠删码，8+3）

表 7-19 对象存储（纠删码，8+3）参考配置

序号	因素	计算公式
A1	存储容量需求（TB）	按实
A2	EC（8+3）	72%
A3	存储使用率水位	85%

序号	因素	计算公式
A4	格式化损耗（容量换算系数）	11%
S1	裸容量需求	S1=A1/A2/A3/(1-A4)
B1	每台服务器 HDD 数量	按实
B2	单 HDD 容量	按实
A5	单台服务器存储（TB）	A5=B1*B2
S2	存储服务器数量（台）	S2=S1/A5（向上取整）（11 台起配）

6、对象存储（元数据服务器，网元、网关服务器配置）

表 7-20 对象存储（元数据服务器，网元、网关服务器参考配置）

序号	因素	计算公式
A1	存储服务器数量（台）	按实
C2	存储节点台数：网关节点台数的典型配比	固定为存储节点比网关节点为 5：1
S1	存储元数据服务器（台）	3P（可用容量）以下不需要 3P-4P（可用容量），配置 3 台 4P-12P（可用容量），配置 5 台 大于 12P（可用容量），配置 7 台
S2	存储网关服务器数量（台）	S2=A1/C2

7、文件存储

表 7-21 文件存储参考配置

序号	因素	计算公式
A1	存储容量需求（TB）	按实
A2	副本数	3
A3	存储使用率水位	85%
A4	格式化损耗（容量换算系数）	11%
A5	文件系统元数据占用	5%
S1	裸容量需求	S1=A1*A2/A3/(1-A4)/(1-A5)
B1	每台服务器 HDD 数量	按实
B2	单 HDD 容量	按实
A6	单台服务器存储（TB）	A6=B1*B2
S2	存储服务器数量（台）	S2=S1/A6（向上取整）（3 台起步）

7.1.3 网络资源

7.1.3.1 网元组件部署

网元节点以虚拟化部署的方式部署在管理服务器上，提供独立的管理和转发能力。网元组件如下：

表 7-22 网元组件

组件	模块	功能
CNP 网元	TGW	转发网关，必选，负责三层转发以及出公网等

组件	模块	功能
	内网通道网关	可选，按需部署；用于虚机监控、安全、windows 虚拟机认证激活等功能
	VxlanGW	裸金属网关，可选，当 TGW 为物理机部署时，可以不需要 VxlanGW
	LBGW	负载均衡网关，可选，按需部署；VPC 级别，不同 VPC 落在不同的网元上。提供负载均衡服务
	VPNGW	VPN 网关，可选，按需部署；VPC 级别，不同 VPC 落在不同的网元上，提供 VPN 网关服务。
控制器	taitan	自研控制器，纳管 CNP 网元和计算节点 OVS
	openflow	Openflow 模块，用于给计算节点 OVS 下发对应流表
	netconf	netconf 模块，调用租户网关或者硬件设备的北向接口下发对应的网络配置
NFVM	NFV-manager	NFV 管理器，负责 CNP 网元生命周期管理
OS 组件	neutron	沿用 neutron 的 API 编排

7.1.3.2 网元服务器选型和参考配置

表 7-23 网元节点服务器参考配置

项目	参考指标
CPU	国产处理器，主频 2.6GHz，核数 48 核，处理器数量 2 颗
内存	≥512GB DDR4
存储	≥2 块 480G SSD 硬盘
网卡	≥4*GE 网口 ≥8*10GE 网口
缓存	≥2GB 缓存，支持缓存数据保护，支持 RAID 0，1，5，6

7.1.3.3 网络设备选型和参考配置

网络设备满足以下要求：

1、云平台内部所需要使用的交换机

业务槽位数≥8 个；主控槽和业务槽之外的独立交换网槽位数≥5 个；交换容量≥2400Gbps；包转发率≥80000Mpps；网络接口≥2 块 48 口千兆电口插卡，≥4 个 1G SFP 端口；独立风扇框数≥3 个，任意风扇框故障或不在位不能造成业务中断。

2、硬件负载均衡

接口至少 2 个万兆光口；并发连接数≥1600 万；4 层每秒新建连接数（CPS）50 万以上，7 层每秒新建连接数（CPS）40 万以上，SSL 每秒新建连接数（CPS）3 万以上；

3、软件级负载均衡

支持包含 TCP 协议和 UDP 协议的四层负载均衡，以及包含 HTTP 协议和 HTTPS 协议的七层负载均衡；支持对应用程序的健康状态检查。

7.2 平台即服务（PaaS）

7.2.1 操作系统

操作系统是用户和计算机之间的接口，同时也是计算机硬件和其他软件之间的接口。操作系统的功能包括管理计算机系统的硬件、软件及数据资源，并控制程序运行，改善人机界面，为其他应用软件提

供支持，让计算机系统所有资源最大限度地发挥作用，提供各种形式的用户界面，使用户有一个好的工作环境，为其他软件的开发提供必要的服务和接口等。在政务行业云中，操作系统运行在国产终端上，管理国产终端系统的硬件、软件及数据资源，并控制程序运行，为业务系统分配运行所需的计算资源。

鉴于政务行业云安全可靠性以及业务系统的特殊性，对服务器操作系统严格要求，主要有以下几个方面：

1、实体一体化的多维主动防护机制，支持多策略的动态加载和动态扩展、全系统客体核内统一可扩展访问控制以及细粒度的强制网络访问控制。

2、核内外协同的高可用故障管理框架，支持低损耗系统服务失效探测、快速故障状态隔离和恢复、用户态透明的状态维护以及基于虚拟化技术的服务快速迁移机制。

3、资源预约的两级混合调度算法，提升实时处理能力，并支持外部中断源与内部定时器协同机制、轻量级事件通信和异步回调机制以及快速中断处理和转发机制。

4、基于硬件抽象层的软硬协同性能优化、基于国产 CPU 的高效能虚拟化平台、基于多核 CPU 资源的任务相关性分解方法，提升基于国产 CPU 整机的计算、存储和显示能力。

目前主流的服务器操作系统包括中标麒麟、统信 UOS、银河麒麟等。

7.2.2 数据库

数据库是依照某种数据模型组织起来并存放二级存储器中的数据集合。数据库中的数据是为众多用户所共享其信息而建立的，已经摆脱了具体程序的限制和制约。不同的用户可以按各自的用法使用数据库中的数据；多个用户可以同时共享数据库中的数据资源，即不同的用户可以同时存取数据库中的同一个数据。数据共享性不仅满足了各用户对信息内容的要求，同时也满足了各用户之间信息通信的要求。

鉴于政务行业云安全可靠性以及业务系统的特殊性，对所选数据库严格要求，主要有以下几个方面：

1、通用性

所选数据库应该支持多种网络协议，包括 IPV4 协议、IPV6 协议等；完全支持 Unicode、GBK18030 等常用字符集，支持多种主流集成开发环境，支持多种开发框架技术，支持国产中间件等。

2、高可用性

当发生系统故障的时候（例如机器掉电），系统通过 REDO 日志，进行重作处理，恢复用户的数据和回滚信息；支持增量备份，支持以检查点进行还原；可备份不同级别的数据，包括数据库级、表空间级和表级；支持在联机、脱机的状态下进行备份、还原操作；采用主备系统提高容灾能力。

3、高性能

采用以字长为分配单位的标准堆栈，提高空间利用率，充分利用 CPU 的 2 级缓存，提升性能；增加栈帧概念，方便实现函数/方法的跳转，为 SQL 脚本的调试提供基础；增加内存运行堆的概念，实现对象、数组、动态的数据类型存储；采用面向栈的表达式计算模式，减少虚拟机代码的体积、数据的移动；重新定义指令系统，增加对对象、方法、参数、堆栈的访问，便于 SQL 的执行；数据批量处理、查询计划重用以及查询结果集的缓存；支持异步检查点模式。

4、高安全性

提供基于用户口令和用户数字证书相结合的用户身份鉴别功能；提供数据库审计功能，审计类别包括：系统级审计、语句级审计、对象级审计；提供实时侵害检测功能，用于实时分析当前用户的操作，并可以查找与该操作相匹配的审计分析规则；提供系统权限和对象权限管理功能，并支持基于角色的权限管理；支持基于 SSL 协议的通讯加密，对传输在客户端和服务器端的数据进行非对称的安全加密，保证数据在传输过程中的保密性、完整性、抗抵赖性；支持对存储数据的透明存储加密、半透明存储加密和非透明存储加密。

5、兼容性

- 体系结构兼容：支持单库单实例结构、表空间—数据文件机制、回滚机制、多版本并发控制等。

- 应用开发接口兼容：支持主流 SQL 语句、OCI/OOCI/OO4O 接口兼容、系统包机制。
- 维护管理方式兼容：支持大量 V$动态视图、AWR 性能分析报告、10053 等事件等。

目前国内主流数据库有人大金仓、达梦、神州通用等。

7.2.3 中间件

中间件是一类连接软件组件和应用的计算机软件，它包括一组服务。以便于运行在一台或多台机器上的多个软件通过网络进行交互。该技术所提供的互操作性，推动了一致分布式体系架构的演进，该架构通常用于支持并简化那些复杂的分布式应用程序，它包括 web 服务器、事务监控器和消息队列软件。中间件在操作系统、网络和数据库之上，应用软件的下层，总的作用是为处于自己上层的应用软件提供运行与开发的环境，帮助用户灵活、高效地开发和集成复杂的应用软件。

鉴于政务行业云安全可靠性以及业务系统的特殊性，对所选中间件严格要求，主要有以下几个方面：

1、集群功能：支持集群功能，队列管理器之间能够共享负载，进行自动负载均衡。

2、动态配置：支持动态配置，可以支持 7×24 小时不间断运行要求，动态配置运行参数。

3、消息队列机制：提供可靠的消息队列机制及独立的队列管理能力，在网络和系统发生故障等各种情况下确保消息不丢、不中。提供网络调度与通讯失败的自动恢复，提供独立于硬件设备实现的网络故障恢复机制，支持异步传输和断点续传。

4、系统安全：遵循国家环境数据交换传输相关标准，支持 Java 2、JAAS、JSSE、JCE、CSlv2 等安全模式和技术。

5、管理监控：支持提供 B/S 结构可视化集中统一监控管理工具。支持对本地和其他远程节点进行统一集中的配置、优化和监控管理，支持远程查看、监控消息中间件、消息及应用的运行状态，支持节点的远程启动和停止。

中间件按类型可分为应用服务器中间件、分布式缓存中间件、分布式消息中间件等，目前国内主流厂商有金蝶、东方通、中创等。

7.2.4 容器云服务引擎

容器云服务引擎（简称 CCSE）提供高度可扩展的、高性能的 Kubernetes 集群、一站式容器服务，兼容主流国产化服务器和操作系统。其整合了镜像、监控、日志、负载均衡、灰度/蓝绿、多种弹性策略、高效调度、集群插件、模板市场等基础能力，帮助企业快速构建和运行可弹性扩展的应用，实现业务的快速交付与持续创新。

容器云服务引擎功能如下：

1、集群管理

- 单集群支持数千节点规模；
- 支持 VM 与容器直连互通；
- 丰富的集群插件，开箱即用。

2、应用管理

- 支持原生 5 种类型工作负载；
- 内置应用模板，支持一键部署 Helm 应用；
- 支持灰度发布，蓝绿发布，应用弹性伸缩。

3、弹性调度

- 支持 HPA/CronHPA 伸缩策略；
- 支持基于历史指标/事件驱动的弹性伸缩；
- 提供负载感知调度，解决原生 k8s 调度不均问题。

4、安全稳定

- 支持 3Master 高可用，镜像服务高可用能力；
- 提供集群备份恢复插件，支持多种存储介质；
- 支持安全容器，提供镜像签名和镜像扫描。

7.3 云管理平台

云管理平台可支持对多种 CPU 架构资源池的统一调度管理，实现对异构计算、存储和网络资源的统一管理。在为用户提供丰富的多元算力，“双云多芯”广泛兼容，安全可靠，面向资源的运维管理、面向资源的服务化过程的运维管理，以及基础设施云的租户和用户管理等，并构建统一的访问门户，实现以上需求的功能化，既对资源的使用者提供资源服务门户，也为资源的管理者提供体验一致的管理能力。

7.3.1 整体架构

图 7-1 云管理平台整体架构

门户管理：支持租户、运营及运维管理门户，通过统一鉴权功能实现各个用户角色权限管控和资源隔离。

资源管理：云资源池的资源管理中心，提供各个资源池中云资源的生命周期管理。

运维管理：提供云资源池、云资源的监控和告警功能，并提供监控大屏进行数据实时展示。

运营管理：提供面向运营人员资源配额、服务目录、事件、工单及业务流程等管理功能

管理中心：管理云管平台自身的系统配置，包括用户管理、权限管理、订单管理和账单管理等。

7.3.2 关键能力

7.3.2.1 双云多芯和异构融合

政务行业领域，在实施信息技术应用创新过程中，针对存量 X86 云资源池与国产化信创资源池共存的情况，混合云管理平台通过广泛的兼容性适配，实现了同一套代码可部署在不同的 CPU 架构服务器，以及对不同 CPU 架构资源池统一管理和统一资源开通。从而降低多云、异构资源池的管理复杂性，屏蔽底层架构差异，实现了“多云多芯，统一管理”。

1、通过多云适配层进行统一模型抽象实现对异构、多云场景的支持。可以通过同一开通页面实现多云资源的开通，避免频繁切换控制台，实现了统一的开通体验。

2、云管理平台具备良好的兼容性，可以部署不同 CPU 架构的服务器上，支持对不同 CPU 架构的资源池进行统一管理，可以通过管理控制台统一开通 X86、ARM 架构的云资源。

7.3.2.2 统一认证和权限管理

统一认证和权限管理，支持多级组织架构管理能力。主要有以下几个方面：

1、支持在各级组织架构管理员下再划分组织架构，以匹配实际组织/租户体系进行管理；各级组织架构管理员都可以分配多个数据中心/地域的资源。

2、通过主账号实现云管的权限认证，通过主账号下挂载子账号实现对平台资源的管理。

3、支持不同云商子账号通过主账号绑定。

4、支持用户在各云平台间切换无感知。

5、采用 RABC（基于角色的权限访问控制）的权限设计，不同角色赋予不同的资源访问权限。

6、统一 Portal 门户包括单点登录 API 网关、系统权限管理中心、签名密钥管理、签名身份认证等几项功能，分别提供用户控制台和管理员控制台。统一 Portal 门户是无状态的，便于部署和弹性扩展。

7、CAS 认证中心包括 CAS 客户端和 CAS 服务端，我们将 CAS 认证需要的数据存储在基础平台，CAS 的客户端和 CAS 的服务端也是无状态的。

8、通过统一认证系统实现所有资源池的登录和认证工作。

9、当用户选择某个平台进行切换时，先判断租户是否在云管理平台中登录。如果没有登录，则要先去统一认证系统中登录。租户在统一认证系统中登录时，先要判断对应的租户是否存在于同一认证系统中。

10、租户在统一认证系统中登录成功后，再进行切换时可以从统一认证系统中拿到对应资源池的认证信息，并通过该认证信息完成租户在资源池间的无缝切换。

11、管理员可管理门户中定义平台的用户角色和各角色的权限范围，并为平台用户授予对应的用户角色，获得相应的用户权限。主要功能包括角色定义和权限分配。

7.3.2.3 计费功能

1、支持针对云计算采集资源使用的数据来计算相关的费用。

2、支持预付费和后付费。

3、支持订单、账单统计和分析概览、用户收支概览、收支明细以及信控管理。

4、支持各种灵活的优惠措施算法：如基本费率依据使用时间长短、容量或者流量自动调整，在一段时间内执行折扣促销。

7.3.2.4 资源和工单管理

1、统一资源管理平台屏蔽底层异构资源池的差异，提供统一的 API 给上层 Console 调用。

2、工单系统负责整个云服务的开发、升级和退订等流程。

3、资源池 SDK 层负责资源池与统一资源管理平台和工单系统的交互，实现统一资源管理平台与资源池的解耦，降低资源池升级对统一资源管理平台的影响。

7.3.2.5 运维监控能力

运维监控支持对虚拟控制中心、可用域、主机、虚拟机、存储池进行监控，能够对云平台下被监控对象的资源使用和业务运行情况进行准确反馈，包含且不限于以下功能：告警管理、监控大屏、统计分析和图形展示、细粒度监控、监控管理和数据管理、日志管理。

7.3.3 功能详情

7.3.3.1 门户管理

云管理平台门户分为自助门户和管理门户：

1、自助门户主要是面向终端用户提供界面，用户可以通过服务门户对服务目录浏览、提交服务请求、实例查询、变更和终止以及对已部署的资源进行控制和统计分析。

2、管理门户主要是面向管理人员提供系统全局管理、服务的设计和变更、服务内容的审查和批准、服务资源开放和审核的入口以及呈现界面。

7.3.3.2 总览管理

1、支持查看待审批的申请、待实施的工单、近期失败的申请、系统异常事件。

2、支持查看近一周申请数据趋势图、近一周登录用户数据趋势图。

3、支持查看系统运行状况，如：虚拟 CPU、虚拟内存、存储的已用和未用数量，物理主机和虚拟机的开机和关机数量。

4、支持查看所有区域或指定区域的所有资源对象，如资源池、集群、主机、存储、网络、虚拟机、虚拟机镜像、虚拟机云磁盘、虚拟机集群。

5、支持通过资源类型过滤资源，如：通过指定虚拟机、云磁盘、镜像、安全组、实例类型等过滤查看。

6、支持查看云平台中使用操作系统以及使用软件的虚拟机数量。

7.3.3.3 服务管理

1、新建编排服务申请、虚拟机服务申请、虚拟机集群申请、云磁盘服务申请、网络服务申请。

2、支持查看权限范围内所有人的申请、某个申请的详细信息、某个申请的任务分解信息。

3、支持以饼状图查看申请状申请的类型。

4、支持查看我的所有工单、待实施的工单、实施中的工单、已完成的工单等。

7.3.3.4 运营管理

1、支持设置开启或关闭虚拟机服务申请权限，如：为部门设置开启创建虚拟机、更新虚拟机、删除虚拟机等。

2、支持以饼状图查看关闭创建虚拟机服务和开启创建虚拟机服务的部门数量、更新虚拟机服务的部门数量、删除虚拟机服务的部门数量。

3、支持为相关部门设置开启或关闭云磁盘服务申请权限，如：创建云磁盘、删除云磁盘、扩容云磁盘等。

4、支持以饼状图显示关闭和开启创建、删除、扩容云磁盘服务部门数量。

5、支持为相关部门设置开启或关闭虚拟机集群服务申请权限；支持以饼状图显示关闭或开启虚拟机集群服务。

6、支持为相关部门设置开启或关闭专有网络申请权限，如：创建专有网络、删除专有网络等。

7、支持以饼状图显示关闭和开启创建、删除专有网络服务部门的数量。

8、支持查看相关部门相应服务的统计数据信息，如：云磁盘服务、虚拟机服务、网络服务、虚拟机集群服务。

9、支持编排服务管理，将云服务能力编排成适合用户申请的云产品，并在产品目录中进行统一展示。如：如创建编排类别、过滤查看编排服务列表。

10、支持添加编排服务，如：通过拖拽图形的方式编排系统、软件资源。

11、支持以饼状图显示编排模板类型比例图。

12、支持显示模板使用频率 TOP5。

13、支持查看我的所有工单、待实施的工单、实施中的工单、已完成的工单等。

14、支持查看审批流程，如：流程名称、流程版本、流程描述、详细操作等。

15、支持为虚拟机资源设置、修改单价。

16、支持设置部门配额，如：为相应部门设置虚拟 CPU，虚拟内存，硬盘等配额。

7.3.3.5 资源管理

云平台可统一纳管 X86、ARM 等异构服务器。

1、支持主机集群管理功能，如：按区域查看、过滤查看主机集群。

2、支持物理主机管理功能，如：查看、过滤查看相关物理主机。

3、支持虚拟机集群管理功能，如：按区域察看虚、过滤察看虚机集群。

4、支持虚拟机管理功能，如：按区域查看、过滤查看虚机；支持以饼状图显示虚拟机统计概要，如虚机开关机状态对比图和虚机的 OS 分布图。

5、支持镜像管理功能，如：上传查看、设置镜像，支持以饼状图显示镜像配置状态图和镜像的 OS 分布图。

6、支持密钥管理功能，如：创建密钥、删除密钥、查看密钥详情、设置密钥用户。

7、支持实例类型管理功能，如：创建、删除、编辑实例类型。

8、支持存储管理功能，如：查看存储资源情况。支持通过过滤框快速搜索指定存储。支持查看存储相关联的主机列表。

9、支持云磁盘管理功能。如，查看云磁盘、设置参数、挂载或解挂载、删除云磁盘。

10、支持网络管理，如：创建、删除、设置网络；支持通过过滤框可以快速搜索指定网络。

11、支持按区域查看路由以及通过管理域筛选条件查看指定路由相关信息。

12、支持查看或通过过滤框搜索指定防火墙。

13、支持 VPC 网络添加、删除、查看功能；支持通过区域，类型和关键字筛选和浏览 VPC 网络。

14、支持添加、删除、修改软件部署服务器。

7.3.3.6 运维管理

1、支持查看资源的实时监控，如：按区域、资源池、数据中心、集群、宿主机、虚拟机等来查看各自的实时使用情况。

2、支持查看计算资源详细信息，如：管理主机数量、负载情况等信息，以及主机对应的 IP、负载情况、CPU/CPU 使用率、内存/内存使用率、硬盘/硬盘使用率、硬盘读写速度、网络下载上传速度、实例数、主机状态等详细信息。

3、支持查看存储资源详细信息，管理存储数量、资源使用情况等信息，以及存储对应的配额使用情况、硬盘总量、硬盘已用、硬盘使用率。

4、支持查看网络资源详细信息，如：管理 IP 数量、资源用量情况、可用 IP 数量、已用 IP 数量。

5、支持查看云平台的历史运行情况，如：按区域、资源池来查看，可按数据中心、集群、主机、时间段等条件查询。

6、支持查看管理域历史监控详情，如：资源历史总览、主机、虚拟机、虚拟机 TOP10 分析。

7、支持查看计算资源历史监控详情，如：计算资源池总览和资源池详细的 CPU/内存使用率。

8、支持查看存储资源历史监控详情，如：存储资源池总览和资源池详细的存储使用率。

9、支持查看网络资源历史监控详情，如：网络资源池总览和资源池详细的 network 总量使用率。

10、支持以部门、项目、申请角度查看相关用户、虚拟机等资源数量。

11、支持通过事件列表查看云管理平台所接收到的事件。

12、支持按时间段、关键字等条件过滤事件列表，支持查询结果导出 Excel 文件。

13、支持配置事件源，如：事件源名称，类型，监控对象等。

14、支持事件阈值配置，如：CPU、Memory、Disk 的报警和紧急的阈值设置。

15、支持任务管理，如：查看任务列表中的主机、虚拟机、网络、安全组等任务信息。

16、支持选择任务的起始时间和类型查询，查看任务详细信息，以及通过结束按钮强行结束正在进行的任务。

17、支持计量统计信息，如：显示虚拟 CPU、虚拟内存、虚拟存储等统计信息。

18、支持按日期或过滤查看统计信息。

19、支持导出 excel 统计报表。

20、支持将现网物理设备统一纳入管理。

7.3.3.7 权限管理

1、支持直接新增用户和从 LDAP 导入用户；支持删除用户；支持修改用户密码。

2、支持查看相关用户的登录用户名、姓名、电子邮件、电话、部门、用户来源等。

3、支持查看用户详细信息，如：使用虚拟 CPU、虚拟内存、硬盘、云磁盘、虚拟机。

4、支持部门管理功能，如：添加、删除、修改部门信息。

5、支持角色管理功能，如：添加、删除角色；支持自定义角色权限。

6、支持项目管理，如：添加、删除项目；支持查看项目详细信息，如：项目中包括的用户名、部门、虚拟机数量。

7、支持环境管理，如：查看环境名称、描述，支持添加、删除环境。

8、支持查看环境中的资源对象状态，如：虚拟机、虚拟机集群。

9、支持职位管理功能，如：添加职位并设置该职位是否有审批权限，支持删除职位功能。

10、支持查看职位详细功能，如：职位名称、是否有审批权限、描述信息、职位中包括的用户的姓名、部门。

7.3.3.8 配置管理

1、支持设置资源池高度策略，如：随机分配、最小负载分配、平均分配、首匹配分配等。

2、支持自定义虚拟机集群扩展策略，如：根据 CPU 和内存使用率扩展虚拟机集群，并可以支持扩展增加或减少虚拟机的数量。

3、支持自定义设置监控指标的定义，如：设置 CPU、内存、存储低用量、正常用量、高用量百分比以及颜色标记。

4、支持添加自定义软件，如：设置虚拟机名称、图标、软件部署方式等。

5、支持添加脚本，如：设置脚本类型为 shell，设置脚本参数等。

7.3.4 与第三方系统对接

云管需提供 OpenAPI 来实现第三方系统接入，实现资源的创建、变配、启停等操作。

计算模块主要提供云主机、镜像、弹性伸缩、裸金属、云主机快照、云主机备份管理接口；存储模块主要提供云硬盘、对象存储、云硬盘快照、云硬盘备份等接口；网络模块主要提供 VPC、子网、安全组、ACL、负载均衡、弹性 IP、NAT 网关对等连接等接口。

云管理平台提供单点登录方式，第三方系统可以云管账号信息进行对接，进行单点登录。

7.4 云迁移

7.4.1 迁移准备

1、对源应用系统进行详细的调研分析，确定所需相应资源及计划迁移方式；
2、在新平台侧准备相应的计算、存储和网络等资源；
3、两侧云平台端对端网络情况；
4、获取相关主机的管理员权限；
5、确定应用系统、数据库的迁移、备份时间窗口、割接时间点等；

7.4.2 迁移场景

通过数据迁移工具把源物理机（虚拟机）的操作系统、应用和设置进行迁移到目标物理机（虚拟机）上，具体有如下 4 种迁移场景，P2P 迁移、P2V 迁移、V2V 迁移、V2P 迁移。

表 7-24 迁移场景

序号	迁移场景	说明
1	P2P	P2P（Physical to Physical）是将物理机转换为物理机的一种技术，即将物理机上运行的操作系统及业务软件完整地迁移到一台新的物理服务器上运行。
2	P2V	P2V（Physical to Virtual）是将物理机转换为虚拟机的一种技术，即将物理机上运行的操作系统及业务软件完整地迁移到虚拟化平台上运行。
3	V2V	V2V（Virtual to Virtual）迁移是在虚拟机之间移动操作系统和数据，如 VMware 迁移到 KVM，Xen 迁移到 vmware；可以通过多种方式将虚拟机从一个 VM Host 系统移动到另一个 VM Host 系统。
4	V2P	V2P（Virtual to Physical）迁移是将虚拟机的操作系统和数据移动到物理机上，如 Xen 迁移到物理机上，即将虚拟机上运行的操作系统及业务软件完整地迁移到一台新的物理服务器上运行。

7.4.3 迁移方式

7.4.3.1 采用迁移同步软件方式

建议采用预先定制虚机模板，再结合专业的迁移同步软件，实现数据同步的方式进行迁移，即在新平台上创建相应版本虚机操作系统的标准虚机模板，启动后，在源、目的虚机上均安装迁移同步工具 agent 的方式，通过旁路式监听源端的数据变化，将源端变化的数据复制到新平台，并将变化的数据实时地传输到远端的新主机，且通过特有的数据序列化传输技术，严格保证源和目的主机数据的一致性和完整性。

7.4.3.2 采用专业迁移工具方式

借助专业的云迁移工具，实现跨主机跨平台的整体迁移，然后再简单调整相关不匹配项的方式，使其适应新平台的虚拟化环境。

特点：此方式对源主机的性能有些影响，且主要是对带宽的大小和稳定性要求较高，迁移的成功率有时偏低，效率不高，将作为项目迁移的次选方案。

7.4.3.3 传统方式

对以上方式均存在问题，不能正常迁移的系统，建议采用通过手工安装主机操作系统、优化配置相关参数、部署应用软件，再将原相关配置及业务数据手工导入主机的方式。

此方式主要用于数据库的迁移。

7.4.3.4 物理迁移

数据库物理迁移是将数据库在原生产环境执行物理备份，再将备份转至目标环境，如云平台，最后在云平台进行恢复从而还原数据库的方法。

7.4.3.5 逻辑迁移

逻辑迁移就是对数据库对象（如用户、表、存储过程等）进行导出，并把逻辑备份文件导入到数据库。

7.4.3.6 文件迁移

1、本迁移方式为通过拷贝数据文件的方式完成数据库迁移，原端停机状态下，将数据文件从原端拷贝到目的端，再将数据库重新启动。

2、拷贝迁移的原端和目的端的文件系统版本与数据库版本都必须一致，进行迁移前原端和目的端的数据库处于关闭状态。

7.4.4 迁移步骤

表 7-25 迁移主要步骤

序号	主要步骤	具体工作
1	充分调研	根据迁移调研表获取现有应用系统的架构、数据容量、资源使用情况、网络架构、IP 策略等信息。
2	编写迁移实施方案	确定数据库迁移方法，规划数据库架构，规划物理主机，云主机，存储以及 IP 规划等，并提交用户审核；
3	实施迁移	采用工具按步骤进行迁移
4	测试验证	对迁移的数据库进行功能和性能测试，对迁移的数据进行验证；
5	业务割接	在数据同步后，进行割接，IP、域名指向等网络割接等工作；
6	值守保障	安排支撑人员现场保障，一般要求至少需要保障 2-3 天

7.4.5 迁移验证

迁移完成后将进行如下验证检查：

- 验证操作系统能否正常启动，并顺畅稳定运行，检查 boot.ini 和 Eventlogs 相关日志无异常、报错信息；
- 确认目标虚拟机的名称，SID 值，确认目标虚拟机的 OS 和 SP 级别。
- 确认目标虚拟机的硬件设备包括 NIC、CPU、RAM 和虚拟磁盘的大小。
- 验证网络连通性、延时、网速和端口开放情况是否正常；
- 验证应用业务端口开放是否正常，并验证等。

7.4.6 应急回退

迁移过程将建议采用专业软件实现源主机在线迁移或手工安装与数据同步软件结合的方式，实现在不中断现有应用业务的同时，在新云平台生成一台完全一样的主机，而原来的主机将继续保留，具体保

留时间可根据实际情况而定。

当新主机出现突发情况，如不能正常启动、数据不准确和访问非常缓慢等异常情况，故障短时间不能立即排除的情况，将可通过 IP 指向或直接使用旧 IP 链接的形式实现应用的快速切换。

7.5 容灾备份

7.5.1 系统功能

云灾备服务平台通过对灾备服务需求和灾备资源整合和匹配，形成云灾备服务的 SLA 和服务目录，为用户提供灾备服务模板。灾备服务目录包括灾备数据类型、灾备时间要求、灾备技术手段、灾备运营服务等内容，以服务的形式向用户提供。用户可根据自己的业务需求进行配置申请。

通过 Web 管理平台，对数据备份恢复进行统一监控管理，设置日常容灾备份策略，所有数据根据设定的规则自动容灾与定期备份；可对所有异地容灾、备份与恢复任务进行监控、审计、报表工作；实现备份与容灾任务邮件报警功能，在备份与容灾任务失败或异常情况，将通过邮件的方式通知管理员。后续新增业务系统可直接纳入集中备份系统的业务系统数据进行统一的保护，确保现有以及将来所有的业务系统数据的安全性。

无人值守的自动策略型恢复演练机制，紧急响应流程，并按计划进行相关的恢复操作演练，验证备份集的可用与有效性。

- 支持重复数据删除，能够实现备份数据在线重复数据删除功能。重删支持全局与局部重删，可灵活定义重删存储池，提升设备利用率；并降低网络带宽要求，减少对生产网络影响，提高备份恢复效率。
- 灵活定义存储池，在管理界面能对新增的磁盘、磁带库设备进行统一管理，可纳入资源池进行管理，可支持存储本地池、共享池、磁带池、重删池；支持全智能数据生命周期管理，按需分层与离线核心备份数据，实现智能生命周期管理。
- 备份按照存储池策略进行保留，可结合时空策略进行保留。并可针对备份时间点数据进行追溯恢复；支持恢复二级索引结构，提高恢复效率。
- 支持数据库、文件备份加速技术，采用优化的存储算法技术，实现对数据备份任务加速。
- 支持备份、恢复断点续传，支持自定义备份作业限速，满足各种恶劣网络环境下的数据备份恢复。
- 基于逻辑回退机制，实现数据库任意时间点恢复。
- 支持包括原机/异机恢复、瞬间挂载恢复与细粒度文件级恢复。
- 支持基于主机应用级实时同步容灾技术，实现应用在线实时同步容灾保护，可一键接管，在线激活。
- 整体运维无需管理人员编写任何脚本与命令，图形化向导方式完成所有运维工作。
- 支持通过增加硬盘等方式实现简单扩容，需要时亦可简单增加存储服务器的数量，提供横向与纵向的灵活扩容方式。
- 多级备份监控管理机制，提供完善与灵活的多级监控功能。

7.5.2 灾备服务级别

云灾备服务平台可将灾备服务资源按单个或多个有机整合的方式发布为云灾备服务目录。云管门户可提供服务配置、服务目录管理功能。对灾备服务的创建和发布、变更、挂起、撤销进行全生命周期管理。当用户申请了灾备服务时，系统将对服务实例的全生命周期地进行管理，如服务申请、操作、变更、终止等功能。

1、备份服务

（1）本地备份

- 应用层备份（APP/FILE/DB/OS）
- 资源层备份（VM/Volume）

（2）跨数据中心备份

- 应用层备份（APP/FILE/DB/OS）
- 资源层备份（VM/Volume）

（3）异地备份（备份数据异地保存和恢复验证）

2、容灾服务

- 应用层容灾（APP/FILE/OS）
- 应用层容灾（FILE 海量非结构化数据文件）
- 应用层容灾（DB）
- 资源层容灾（VM/Volume）

灾难系统一般由可接替生产系统运行的后备运行系统、数据备份系统、备用通讯线路等部分组成，通过统一的云灾备管理平台，建立并制定了一系列运行管理制度、数据备份策略和灾难恢复程序，确保在灾难发生后，关键数据、数据处理系统和业务系统在短时间内能够恢复的过程。

7.5.3 灾备服务内容

表7-26 灾备服务内容

服务类型	服务内容	说明
备份基础服务	云主机 APP&文件定时备份	采用客户端代理方式，通过制定备份策略，保护 APP 应用和文件数据，实现多副本历史时间点的数据恢复
	云主机 DB 数据库定时备份	采用客户端代理方式，通过制定备份策略，保护 DB 数据库应用数据，实现多副本历史时间点的数据恢复
	云主机 DB 数据库连续日志备份	采用客户端代理方式，通过制定备份策略，保护 DB 数据库应用数据，基于日志回滚的数据库任意时间点恢复技术，遇到数据库逻辑故障，可恢复到历史任意时间点，可保证恢复状态的有效性
备份高级服务	云主机整机定时备份	通过制定备份策略，保护云主机操作系统和磁盘数据，实现多副本历史时间点的云主机整机恢复
	单台云主机整机实时备份	保护单机整机备份，包括操作系统、应用、数据、磁盘数据卷，既可应对普通数据丢失，也能对整机完全瘫痪情况作回退修复
	海量非结构化数据备份归档	采用对象存储，通过制定复制策略，保护海量非结构化音视频、图像和文件数据，实现数据副本的在线访问，需要购买咨询服务制定支持方案
	物理主机操作系统定时备份	保护操作系统，实现系统整体快速恢复或异机迁移
容灾高级服务	云主机 DB 数据库实时容灾	采用基于日志的结构化数据同步技术，按照主机业务系统事务顺序实施数据同步，保障备机数据库与主机数据库的事务级完整性和一致性，实现业务系统快速切换和恢复
	云主机整机实时容灾	支持整机灾难接管，支持热备接管和冷备接管两种方式

7.6 云资源池安全

7.6.1 云平台安全

云平台本身必须满足国家信息系统安全等级保护三级要求。

云平台安全包括但不限于如下：网络安全审计、数据库审计、日志审计、漏洞扫描、堡垒机、态势感知平台、探针和 APT 检测系统等。

1、网络安全审计

具备系统级审计、应用级审计和用户级审计能力，按照一定的安全策略，利用记录、系统活动和用户活动等信息，检查、审计和检验操作事件的环境及活动，从而发现系统漏洞、入侵行为或改善系统性能，审查评估系统安全风险，记录与审查用户操作计算机及网络系统活动过程，规避数据安全事件和违规上网行为。

2、数据库审计

支持国产数据库，从保障数据库应用安全的角度进行设计，以网络数据捕获能力、数据库协议解析、事件关联分析为基础，可以精准识别数据库操作以及采取各种响应行为。

3、日志审计

具备日志监控、日志采集、日志存储、日志检索、日志分析等能力，支持国产操作系统、网络设备、安全设备、应用系统等，满足各个单位对合规性要求的日志审计。

4、漏洞扫描

具备系统扫描、Web 扫描、主机扫描、端口扫描、弱口令破解、配置指标检查、OS 识别、漏洞检测数据采集、多重服务检测、安全优化扫描等能力。

5、堡垒机

实现对网络设备、数据库、安全设备、主机系统、中间件等资源统一运维管理和审计，具备账号管理、身份认证、资源授权、访问控制、操作审计等能力。

6、态势感知平台

从流量探针、终端、安全设备和第三方网络设备处收集流量和日志数据，提供威胁攻击分布、威胁事件态势、最新威胁事件、风险趋势等能力；

7、探针

通过对流经该关键路径上的网络数据流进行 L4~L7 层的深度分析，实时检测黑客、木马、蠕虫、病毒、间谍软件、协议异常、DoS/DDoS 等网络攻击，发现用户异常流量行为等异常。

8、APT 监测系统

具备文件内容分析特征库分析引擎，支持对多种文件类型进行检测，发现勒索病毒、木马、挖矿病毒等恶意代码。

7.6.2 租户安全

除上述云平台基本安全要求外，应提供虚拟防火墙、WAF 服务、WEB 防篡改、主机漏洞检测服务、主机防病毒服务、数据库审计和日志审计等租户安全服务。

1、虚拟防火墙

具备安全策略、静态路由、动态路由、策略路由、NAT、报文攻击防护、多种 DoS/DDoS 攻击防护、ARP 攻击防护等能力，支持针对 HTTP、SMTP、IMAP 等协议和应用的攻击检测和防御，支持对 telnet、SMTP、FTP 协议的暴力破解防护。

2、WAF 服务

具备识别并防止跨站脚本（XSS)、注入式攻击（包括 SQL 注入、命令注入、Cookie 注入等）、跨站请求伪造等应用攻击行为，并过滤掉某些可能让应用遭受 DOS（拒绝服务）攻击的流量。

3、主机漏洞检测服务

具备全面发现信息系统存在的各种脆弱性问题，包括安全漏洞、安全配置问题、应用系统安全漏洞，检查系统存在的弱口令，收集系统不必要开放的账号、服务、端口，形成整体安全风险报告。

4、WEB 防篡改服务

对网站服务器提供安全防护，作为针对网站服务器的各类访问请求进行检测和验证。确保其安全性和合法性，对非法的请求予以实时阻断，防止网页被篡改，从而对各类网站站点进行有效防护。

5、主机防病毒服务

具备蠕虫或者木马等常见病毒的检测与查杀，包括清除、隔离以及自动地排除，提供病毒隔离，将染毒文件安全隔离并备份，可以从隔离区中对染毒文件进行恢复。防止误操作或异常情况下造成的文件损失，为用户提供病毒文件恢复机制。

6、日志审计服务

具备日志监控、日志采集、日志存储、日志检索、日志分析等能力，支持国产操作系统、网络设备、安全设备、应用系统等，满足各个单位对合规性要求的日志审计。

7、数据库审计

支持国产数据库，从保障数据库应用安全的角度进行设计，以网络数据捕获能力、数据库协议解析、事件关联分析为基础，可以精准识别数据库操作以及采取各种响应行为。