广东省“数字政府”政务云平台建设规范

（征求意见稿）

目 次

引　言

为了加快推进“互联网+政务服务”体系的建设，推进政务信息化建设体制改革，根据《广东“数字政府”改革建设方案》（粤府〔2017〕133号）《广东省“数字政府”建设总体规划（2018-2020）》（粤府〔2018〕105号）的要求，“数字政府”将按照“管运分离”的管理架构、“整体协同”的业务架构、“集约共享”的技术架构进行规划建设，构建“1+N+M”的全省一片云。

本规范主要是针对政务云平台部分的建设，通过统一规划、统一建设、统一运营，实现云资源的集约共享，支持上层业务应用的整体协同，保证全省“数字政府”的可持续发展。

1 范围

本规范适用于广东省内新建的“数字政府”政务云平台，以及现有政务云平台升级改造的规划设计、设备选型、建设实施等，具体技术细节另行发文规定。

2 规范性应用文件

下列文件对于本文件的应用是必不可少的。凡是注明日期的引用文件，仅注日期的版本适用于本文件。凡是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。

ISO/IEC 17788 信息技术 云计算 概述和词汇

GB/T 31167 信息安全技术 云计算服务安全指南

GB/T 31168 信息安全技术 云计算服务安全能力要求

GW0013 国家电子政务外网标准 政务云安全要求

3 术语、定义和缩略语

下列术语和定义适用于本文件。

3.1 政务云 Government Cloud

用于承载各级政务部门开展公共服务、社会管理的业务信息系统和数据，并满足跨部门业务协同、数据共享与交换等的需要，提供 IaaS、PaaS 和 SaaS 服务的云计算服务。

3.2 云服务客户 Cloud Tenant

在政务云中，云服务客户指使用政务云的各级政务部门，即使用政务云开展电子政务业务和处理、存储数据的组织

（或机构）及相关事业单位。包括单位内部业务使用人员及对云相关云资源和安全的管理人员。

3.3 云服务方 Cloud Service Party

管理、运营、支撑云计算的计算基础设施及软件，通过服务方式将云计算的资源交付给客户。在政务云中，云服务方指为各级政务部门提供计算、存储、网络及安全等各类云计算基础设施资源、相关软件和服务的提供商，及负责执行云服务方业务运营和相关管理工作。

3.4 政务云管理单位 Government Cloud Management Unit

政务云的行政监管单位，负责政务云平台的规划、应用、监督、管理及对云服务方的考核，审核云服务客户的政务云平台使用需求，受理政务云平台建设方案备案及服务费用的审核。

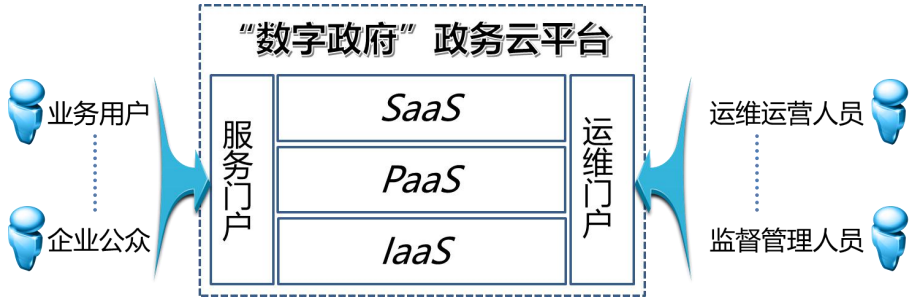
4 总体概述

4.1 总体架构

4.1.1 服务框架

“数字政府”政务云平台以“互联网+政务服务”技术体系、政务云安全要求、云计算服务安全指南等国家标准为依据进行总体架构构建。本规范主要是对基础设施即服务（IaaS）、平台即服务（PaaS）、软件即服务（SaaS）、云管理平台等进行阐述。平台涉及的安全体系、灾备体系等在对应的规范中另行规定。

各层服务的要求和描述如下：



1、IaaS 层：基础设施即服务层，向政府用户提供计算、存储、网络等资源服务，提供访问云基础设施的服务接口等，以及 IaaS 层的安全服务。

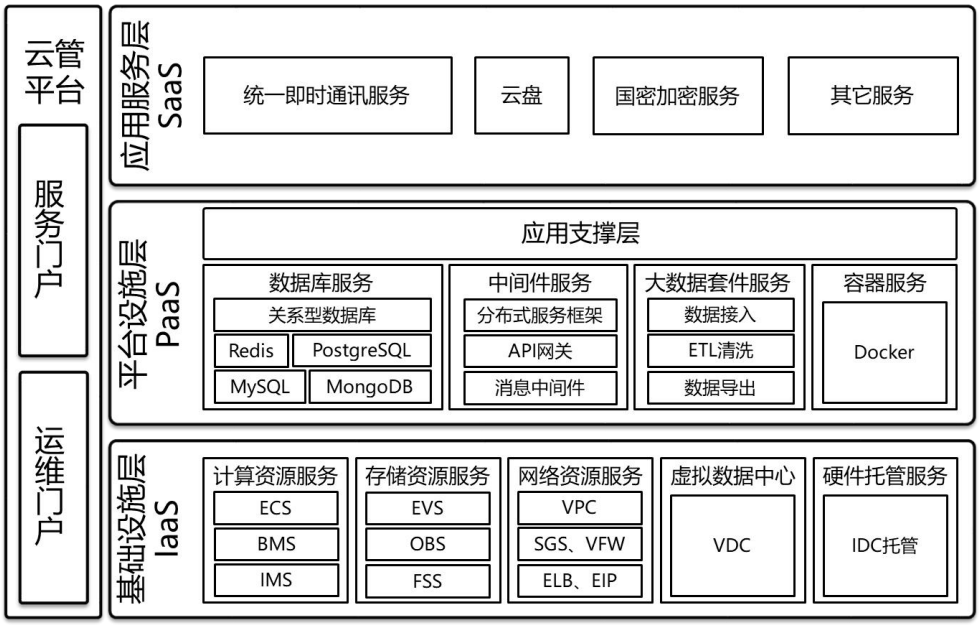
2、PaaS 层：平台即服务层，向政府用户提供运行在云基础设施层之上的软件开发和运行平台服务，以及 PaaS 层的安全服务。实现该层所需要的计算、存储、网络等资源由 IaaS 层统一提供。

3、SaaS 层：软件即服务，向政府用户提供运行在云基础设施之上的应用软件，以及 SaaS 层的安全服务。实现该层所需的计算、存储、网络等资源由 IaaS 层统一提供。

4、服务门户：向政府管理层、业务用户、企业公众等提供全省风格统一的访问入口。对全省政务云平台的使用情况、运行情况等进行统一呈现。

5、运维门户：向政府管理层、业务用户、运维运营主体等提供运维、运营的平台服务，以及为政务云平台管理单位提供准确的平台运维数据，支撑其进行各项运维、绩效指标考核。

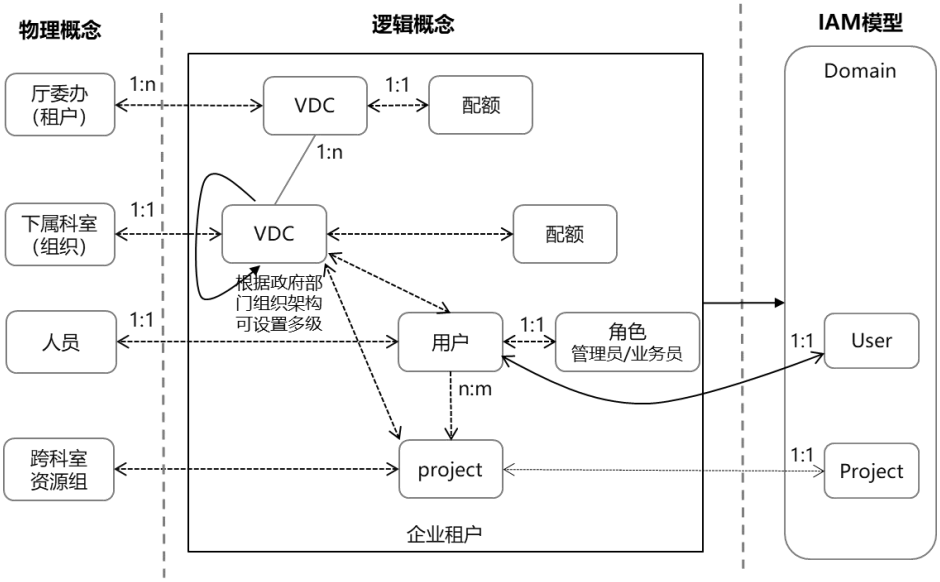
整体服务框架如下:



4.1.2 组织框架

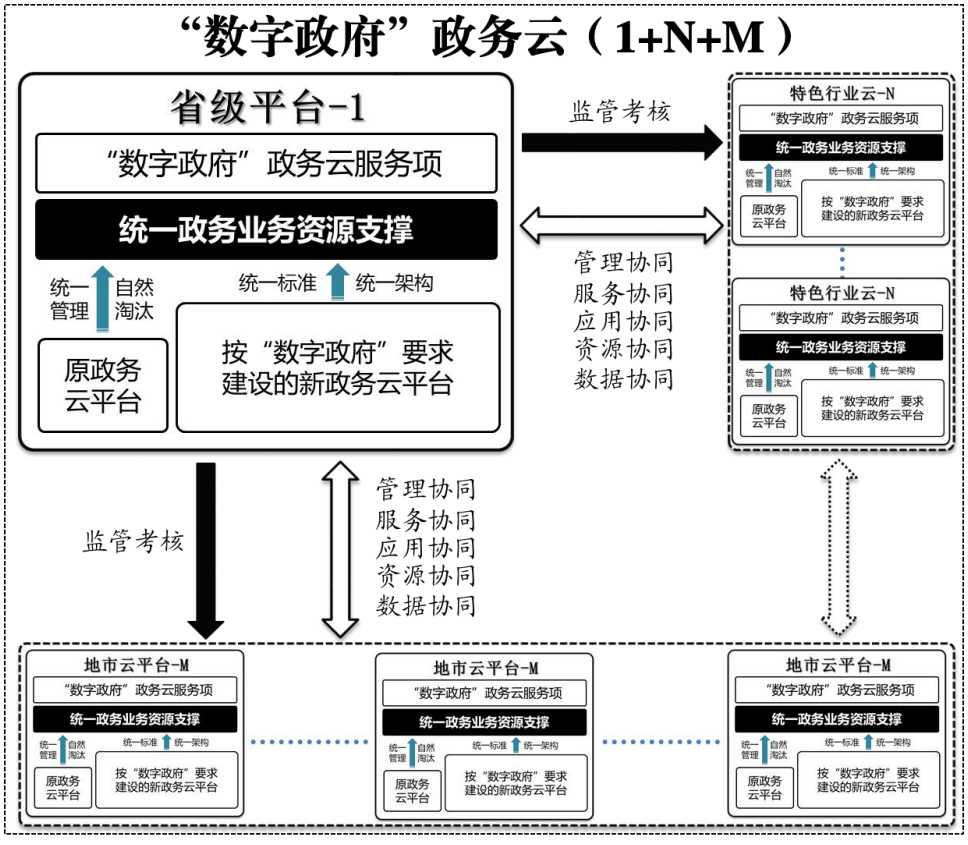
“数字政府”政务云平台将根据政府部门的组织架构，采用多级权限体系，下级权限来自于上级的授权。各级权力主体需要对权力范围内的整体情况负责及向下授权，是上一级权力主体的考核主体。

每个委办局对应一个资源组织，内置多级 VDC 对就各委办局下属的不同业务科室或业务项目组。每个部门可以设置配额，对应部门对资源的预算。每个 VDC 设置一个管理员，负责本级及下级 VDC 的用户和资源。



4.2 总体要求

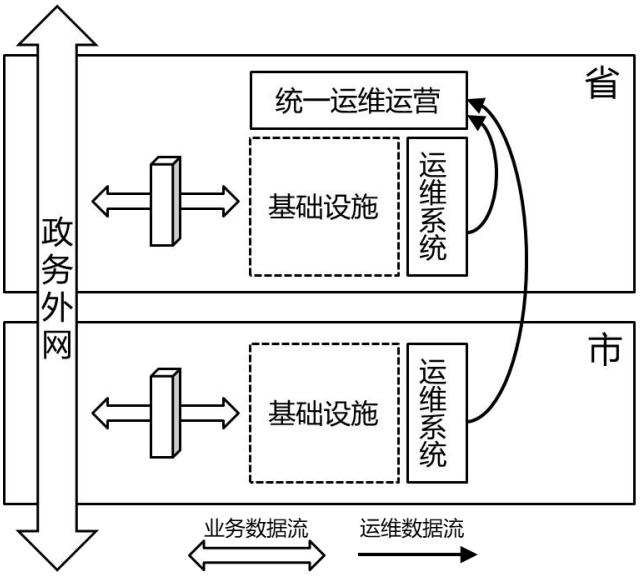
全省“数字政府”云平台需要按照统一的架构进行建设，并由省里进行统一的监管考核。同时，为实现全省一片云，省市之间要做“五协同”：管理协同、服务协同、应用协同、资源协同、数据协同。



4.2.1 管理协同

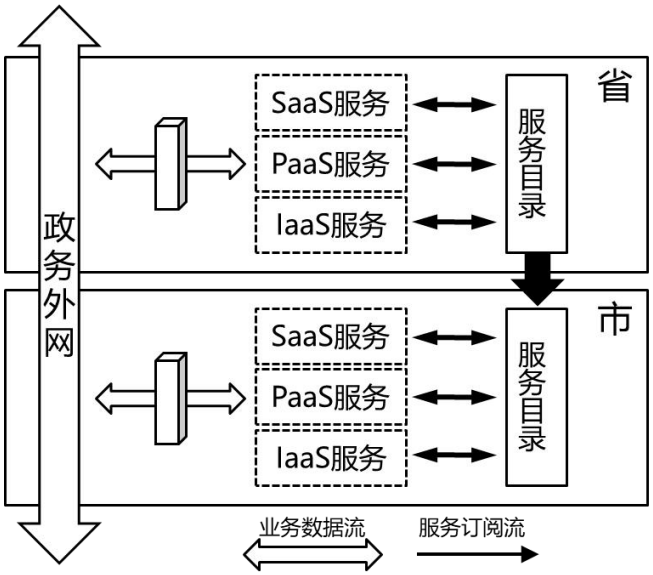
省级对全省各个地市的云进行统一的运行监控。

在省级的运维管理界面上统一呈现省本级以及各个地市的各类资源的统计数据、资源池容量数据、告警汇总和概要数据等，实现全省一片云的统一监控。各级运维平台北向提供统一 API 接口，上一级运维平台通过这些接口获取各级物理资源、云平台资源、大数据平台资源的统计信息以及详细信息，并根据具体呈现要求统一分析呈现。



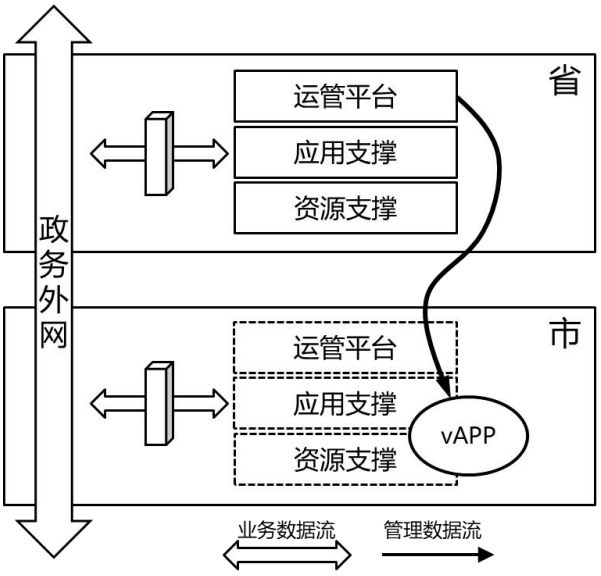
4.2.2 服务协同

全省基于统一架构建设，提供的一致的服务项、一致的计量标准、一致的计费标准。把第三方的应用封装全省共用的服务，包含服务的上架、发布、审批、订购、更新、绑定、下架、删除等全流程。省统筹的服务目录能够快速在地市统一发布和按需申请。



4.2.3 应用协同

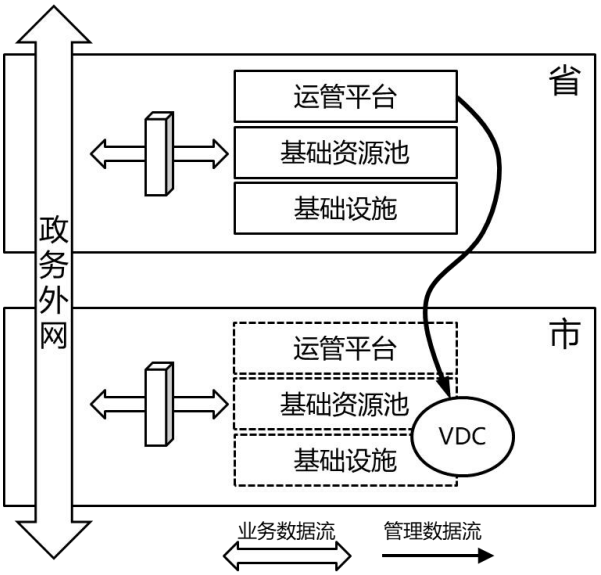
当需要在全省统一快速部署各类业务应用时，可以将业务应用打包成标准的应用快速安装镜像，推送到全省一键式快速部署上线。



4.2.4 资源协同

当需要统一推进业务部署及统一协调资源时，可以从省里直接向市平台调用资源，实现省市逻辑统一、物理分散、资源灵活使用和调度。各级资源平台使用统一平台技术规范、

业务上云规范管理、北向接口规范。



4.2.5 数据协同

政务数据中心包含了不同数据源的海量数据，且这些数据可能分布在不同的数据中心。协同计算是一个兼容相同数据中心和跨数据中心多数据源协助查询的系统，支持下推计算任务、基于代价的优化方式、数据传输加速等功能；打破数据流通障碍，即时利用异地集群数据协同分析。

1、对于数据分散在多个数据源、多个地域的情况，支持跨地跨数据源查询分析，支持统一 SQL 接入和查询。

2、对于跨地跨数据源的查询分析，提供 JDBC 访问接口。

3、对于跨地跨数据源的查询分析，提供数据表的可视化管理界面。

4、对于数据分散在省、市多朵云内的协同查询，需满足政务行业的对 DSA、VPN、网闸等基础环境的要求。

5 IaaS 平台建设要求

5.1 总体要求

建设基于 OpenStack 框架的 IaaS 云服务资源池，实现基础设施资源的统一管理。通过虚拟化平台和分布式数据中心管理平台，形成逻辑统一的资源池，为各委办局单位提供统一的计算资源服务、存储资源服务、网络资源服务、虚拟数据中心服务、硬件托管服务等 IaaS 层服务。

5.1.1 技术架构

政务云平台 IaaS 层主要由硬件设施、资源池层、服务层组成:

1、硬件设施

IaaS 层的基础是各种硬件设施,主要包括服务器、存储、网络、负载均衡、防火墙等硬件设备。

2、资源池层

资源池层将硬件整合成计算资源池、存储资源池、网络资源池等。各种资源池可以根据项目需要进行构建和裁剪。

3、服务层

服务层通过对资源池层各类资源的封装，实现云资源服务的发现、路由、编排、计量、接入等功能，显现从资源到服务的转换。

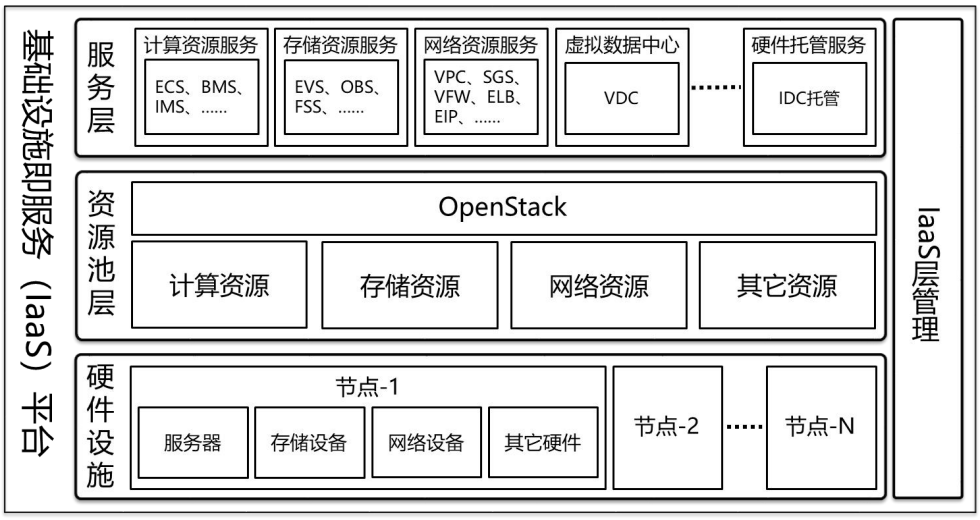
主要包括计算资源服务（虚拟机服务 ECS、物理机服务 BMS、镜像服务 IMS 等）、存储资源服务（块存储服务 EVS、对象存储服务 OBS、文件存储服务 FSS 等）、网络资源服务（虚

拟私有云 VPC、安全组服务 SGS、虚拟防火墙服务 vFW、弹性负载均衡 ELB、弹性 IP 服务 EIP 等)、虚拟数据中心(VDC)、硬件托管服务等。

4、IaaS 管理层

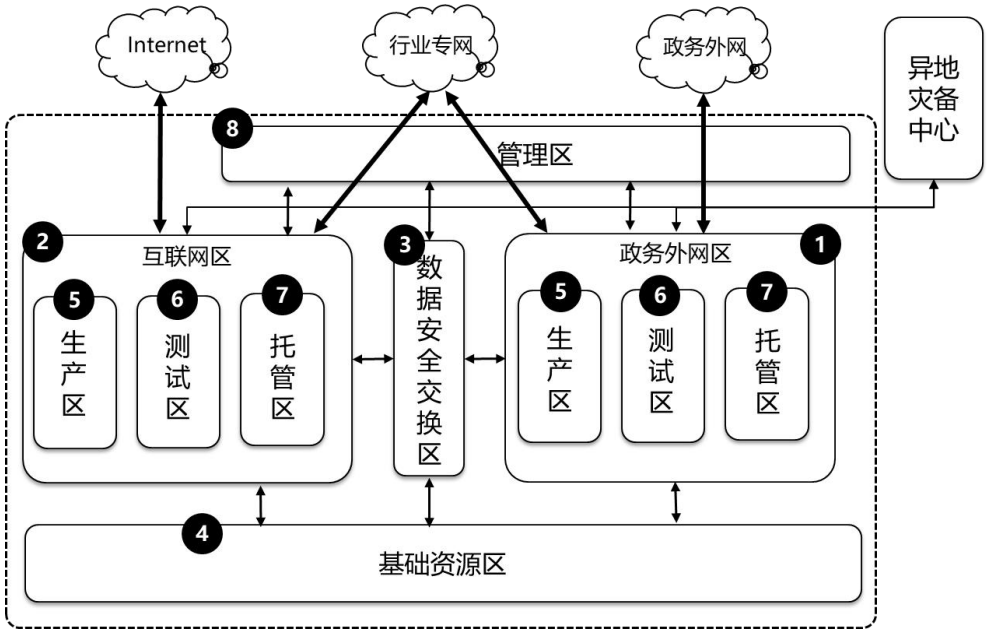
IaaS 层的整体运维管理及公共组件的管理平台，包括 VDC 管理、租户管理、服务目录、服务控制台、计量、资源管理、告警管理、拓扑管理、性能管理以及统计报表等。

总体技术架构示意如下:



5.1.2 业务分区

从业务界面上，“数字政府”政务云整体分为政务外网区和互联网区，两个业务区构建单独的物理资源池，物理网络相互隔离。每个区域内至少要划分生产区、测试区和托管区。



1、政务外网区：承载政务外网业务，包括各委办局专业业务，只能通过政务外网进行访问。

2、互联网区：承载政务直接面向公众用户的业务系统资源区，可通过互联网进行访问。

3、数据安全交换区：对互联网区和政务外网区进行数据交换，也要进行数据的清洗和脱敏等处理。

4、基础资源区：提供计算、存储、网络、安全等基础资源。

5、生产区：承载正式上线的生产系统。

6、测试区：系统上线前的开发和测试区域，原则不允许外部访问。

7、托管区：承载政务行业专网中具有特殊要求的业务应用。

8、管理区：提供统一的安全、运营运维、灾备等管理系统。

5.2 服务要求

5.2.1 计算资源服务

计算资源服务至少包含虚拟机服务、物理机服务、镜像服务等。

服务 SLA 要求如下:

序号	服务类型	响应时间	交付时间	服务可用性	数据可靠性
1	物理主机服务	≤30 分钟	1 个工作日	≥99.95%	99.9999%
2	虚拟主机服务	≤30 分钟	1 个工作日	≥99.95%	99.9999%
3	镜像服务	≤30 分钟	1 个工作日	≥99.95%	99.9999%

5.2.1.1 虚拟机服务（ECS）

1、服务定义

虚拟机服务（Elastic Compute Service）是一种弹性可伸缩的计算服务，有利于降低 IT 成本，提升运维效率。虚拟机可以使用户在几分钟之内迅速地获得虚拟机设施，并且这些基础设施是弹性的，可以根据需求进行扩展和收缩。

序号	类型	参考规格
1	基础型	2 核、4G 内存、100G 硬盘
2		4 核、8G 内存、100G 硬盘
3	通用型	8 核、16G 内存、100G 硬盘
4		16 核、32G 内存、100G 硬盘
5	内存型	2 核、8G 内存、100G 硬盘
6		4 核、16G 内存、100G 硬盘
7		8 核、32G 内存、100G 硬盘
8		16 核、64G 内存、100G 硬盘
9	计算型	32 核、64G 内存、100G 硬盘
10		32 核、128G 内存、100G 硬盘

11	定制化	定制化虚拟机服务（2 vCPU/单位）
12		定制化虚拟机服务（4G 内存/单位）

2、服务要求

（1）要求指定云服务器类型和规格（Flavor）创建云主机，支持根据预制的多种类型的云服务器类型供选择，针对不同的应用场景，可以选择不同规格的弹性云服务器。

（2）要求使用公共镜像发放 VM，公共镜像由系统管理员制作并注册到系统中，一般提供常见的标准操作系统镜像，所有用户可见。包含操作系统以及预装的公共应用。

（3）要求使用私有镜像或共享镜像发放 VM，私有镜像服务用于满足用户个性化需求。选择私有镜像创建云主机，可以节省重复配置云主机的时间。私有镜像仅用户自己可见。包含操作系统、预装的公共应用以及用户的私有应用。用户可基于 ECS 实例或者已有的镜像文件创建的私有镜像。

（4）要求 ECS 实例计量，支持计量实例 vCPU 和内存信息。

（5）要求支持用户查看 VM 的动态信息，包括 CPU 使用率、磁盘读速率、磁盘读操作速率、磁盘使用率、磁盘写速率、磁盘写操作速率、内存使用率、带内网络流入/流出速率、带外网络流入/流出速率。以及要求查询 VM 静态信息，包括 CPU 核数、内存、IP/VPC/网卡所在的网络/安全组。

5.2.1.2 物理机服务（BMS）

1、服务定义

物理机服务（Bare Metal Server，裸金属服务器）为政务云用户承载一些重载类业务，如数据库、核心业务系统、大数据等，同时实现网络的自动化配置。裸金属服务器不运行虚拟化层，直接安装用户 OS。对于不适合 VM 部署的应用可以使用裸金属服务器服务。

序号	类型	参考规格
1	物理服务器 I 类	CPU：4 路 16 核，主频 2.10GHz，或同等性能配置 内存：512G 硬盘：2 块 900G SAS 硬盘，或同等容量配置 接口：16G HBA 卡、万光网卡
2	物理服务器 II 类	CPU：2 路 10 核，主频 2.20GHz，或同等性能配置 内存：256G 硬盘：2 块 900G SAS 硬盘，或同等容量配置 接口：16G HBA 卡、万兆网卡

2、服务要求

（1）支持将物理服务器定义成服务目录供用户申请使用，用户可以根据自己的需要选择物理机规格、镜像，并且能够实现自动化完成卷挂载、安装软件、网络配置等工作。

（2）要求 X86 服务器作为裸金属服务资源池，单 region 支持 256 台主机，支持挂载 EVS 服务做为数据卷，用户可以选择裸金属服务规格，可查询静态信息，包括 CPU 核数、内存、IP/VPC/网卡所在的网络。

（3）要求 BMS 云服务的生命周期管理，包括启动、关机、重启、删除等。支持 BMS 实例计量，支持计量实例 CPU 和内存信息。

5.2.1.3 镜像服务（IMS）

1、服务定义

镜像服务（Image Management Service）是弹性云主机实例可选择的运行环境模板，一般包括操作系统和预装的软件。通过镜像，可以在弹性云主机实例上实现应用场景的快速部署。

私有镜像用于满足用户个性化需求。选择私有镜像创建云主机，可以节省重复配置云主机的时间。私有镜像仅用户自己可见。包含操作系统、预装的公共应用以及用户的私有应用。用户可基于 ECS 实例或者已有的镜像文件创建的私有镜像。

2、服务要求

（1）通过弹性云主机创建私有镜像服务，可以通过弹性云主机，生成私有镜像。系统支持最大镜像数 200 个。已有镜像文件创建私有镜像服务，可以把对象存储服务桶中的镜像文件注册为私有镜像。

（2）用户可以在创建 ECS 实例时选择私有镜像，修改镜像名称、描述，创建 ECS 实例时可以选择被共享镜像，支持把对象存储服务桶中的私有镜像文件下载到本地。可以指

定下载镜像格式 zvhd、vhd、Qcow2、VMDK，支持计量私有镜像个数，设置每个 Project 的 IMS 实例个数配额。

5.2.2 存储资源服务

存储资源服务至少包括块存储服务、对象存储服务、文件存储服务。

服务 SLA 要求如下:

序号	服务类型	响应时间	交付时间	服务可用性	数据可靠性
1	块存储服务	≤30 分钟	1 个工作日	≥99.95%	99.9999%
2	对象存储服务	≤30 分钟	1 个工作日	≥99.95%	99.9999%
3	文件存储服务	≤30 分钟	1 个工作日	≥99.95%	99.9999%

5.2.2.1 块存储服务（EVS）

1、服务定义

块存储（Elastic Volume Service，又称云硬盘）可以独立于云主机的生命周期，挂载到同一可用分区下的云主机或者从云主机上卸载。用户申请云主机时可以指定容量大小、存储 SLA。至少提供普通 IO 云硬盘、高 IO 云硬盘、超高 IO 云硬盘等。

序号	服务名称	参考规格
1	普通 IO 云硬盘（100G/单位）	适用于大容量、读写速率中等、事务性处理较少的应用场景。单盘最大 IOPS 为 800。
2	高 IO 云硬盘（100G/单位）	适用于主流的高性能、高可靠应用场景。单盘最大 IOPS 为 2500。
3	超高 IO 云硬盘（100G/单位）	适用于超高 IO，超大吞吐量的读写密集型应用场景。本期单盘最大 IOPS 为 10000。

2、服务要求

（1）支持用户自助管理，包括创建、挂载、卸载、删除:

◎创建单个空白云硬盘：用户可以创建一块云硬盘。

◎挂载云硬盘到云主机：用户可以将一块云硬盘挂载到某个弹性云服务器上。

◎从云主机卸载云硬盘：用户可以把一块已经挂载的云硬盘进行卸载。

◎删除单个云硬盘：用户可以删除一块云硬盘。

（2）支持不同类型（普通 IO、高 IO、超高 IO）的 EVS 磁盘，用户可以根据应用场景对 IO 的需求进行选择;

（3）弹性扩容可以随时根据用户的需求扩展磁盘的容量，满足不断增长的业务对更多存储容量的需求;

（4）单块系统磁盘大小支持 1GB-32TB，数据盘大小支持 1GB-32TB,最大限度满足用户对不同存储容量云硬盘的需求。

5.2.2.2 对象存储服务（OBS）

1、服务定义

对象存储服务（OBS，Object Storage Service）是一个基于对象的海量存储服务，为客户提供海量、安全、高可靠、低成本的数据存储能力，包括：创建、修改、删除桶，上传、下载、复制、修改、删除对象等。

2、服务要求

对象存储服务提供海量、安全、高可靠、低成本的数据存储能力，支持至少 5TB 的超大文件存储。

（1）支持创建、删除、查看桶和 AK/SK 密钥。支持桶 ACL 设置、对象 ACL 设置和桶策略设置;

（2）支持存储资源池在线扩展;

（3）支持数据检查：存储前一致性检查，确保存入数据是上传数据;

（4）支持全局命名空间，无需指定 region 即可访问全部桶和对象;

（5）生命周期管理：用户可以为某个桶定义生命周期管理规则，来为该桶的对象定义各种生命周期规则;

（6）支持查看用户配额（容量）、桶配额（容量）;

（7）支持最大 5TB 的超大文件存储;

（8）多版本控制：开启多版本控制后上传对象时，OBS 自动为每个对象创建唯一的版本号；上传同名的对象将以不同的版本号同时保存在 OBS 中。可以指定版本号下载对象，不指定版本号默认下载最新的对象。

（9）支持大文件分段上传和合并。

（10）批量删除对象。

5.2.2.3 文件存储服务（FSS）

1、服务定义

文件存储服务（File Storage Service）开通文件存储空间，可用于不同类型计算机、操作系统、网络架构和传输协议运行环境中的网络文件远程访问和共享。

文件存储服务具备高可用性和持久性，为海量数据、高带宽型应用提供有力支持，适用于多种应用场景，包括媒体处理、文件共享、内容管理和 Web 服务等。

2、服务要求

（1）单一文件系统存储容量可扩展至≥100PB。

（2）支持 NFS（V3/V4），SMB（V1/V2/V3），HDFS（支持与 Cloudera 对接），FTP，NDMP，Amazon S3/OpeanStack Swift 接口。

（3）支持单客户端对多个节点并发访问，单客户端最大带宽可达 2.5GBps。

（4）支持并配置客户端连接负载均衡软件，负载策略支持 CPU 占用率。支持自动精简配置，可按需动态分配存储空间，保证存储资源的最大化利用。

（5）支持文件系统标准的目录/文件权限操作，支持用户/组的读/写/执行权限。

5.2.3 网络资源服务

网络资源服务至少包括虚拟私有云服务、安全组服务、虚拟防火墙服务、弹性负载均衡服务、弹性 IP 服务等。

服务 SLA 要求如下:

序号	服务类型	响应时间	交付时间	服务可用性
1	虚拟私有云	≤30 分钟	1 个工作日	≥99.95%
2	安全组	≤30 分钟	1 个工作日	≥99.95%
3	虚拟防火墙	≤30 分钟	1 个工作日	≥99.95%
4	弹性负载均衡	≤30 分钟	1 个工作日	≥99.95%
5	弹性 IP	≤30 分钟	3 个工作日	≥99.95%

5.2.3.1 虚拟私有云（VPC）

1、服务定义

虚拟私有云（Virtual Private Cloud），用于帮助用户在云中虚拟出一个私有的应用运行环境和安全域。

VDC 业务管理员可以在 VPC 中定义与传统网络无差别的虚拟网络。VDC 业务管理员创建 VPC 后，可以在 VPC 内申请路由器、网络（DHCP、DNS 等）、弹性 IP、SNAT、ACL、安全组、VPN 等高级网络服务，以满足更多的业务部署要求。

每个 VDC 至少有一个 VPC，且允许申请多个 VPC，VPC 之间网络空间隔离，可按业务安全隔离要求规划 VPC。每个 VDC 内最多可支持 500 个 VPC。

2、服务要求

（1）支持多个子网，支持 SNAT

使用 1 个公网 IP 满足虚拟机访问 internet 的需求，节省公网 IP;

（2）VPC Peering

支持租户使用私有业务 IP 地址在安全隔离的 VPC 之间实现三层路由互通;

（3）管理方面要求

管理方便，用户可以通过 web 页面或者开放 API，同时管理大量 VPC 实例;

（4）安全方面要求

完全控制，用户可以完全控制自己创建的 VPC 实例。

5.2.3.2 安全组服务（SGS）

1、服务定义

虚拟机可以加入安全组，安全组用来实现组内和组间的访问控制，加强虚拟机的安全保护，实现 VPC 内部的网络隔离。

2、服务要求

（1）安全组服务保证虚拟机的安全，提供虚拟机粒度的安全访问控制。

（2）安全组控制云主机网络消息的流入流出，只运行授权的消息通过。

（3）当云主机申请成功后，可以将云主机加入到某个安全组内，安全组上配置安全规则。

（4）可以将 VPC 内的虚拟机加入一个安全组，然后设定不同安全组间的访问规则。

（5）同一个安全组内的地址之间的访问不受限制，默

认组间是禁止访问的。

5.2.3.3 虚拟防火墙服务（VFW）

1、服务定义

将物理防火墙虚拟成逻辑上互相独立的多台防火墙（适用于纯硬件 Overlay 网络方案），为用户的网络设备和应用提供防火墙安全服务。

2、服务要求

为用户提供安全访问控制服务，保证用户应用的安全性。

虚拟防火墙服务支持在逻辑上将物理设备划分成多个虚拟域（VDOM），而每个虚拟域（VDOM）均可以看成是一台完全独立的防火墙设备，彼此之间互不干扰，并拥有独立的系统资源、接口、路由表、会话表、安全配置策略、用户管理等，为用户账户下具有公网 IP 地址的虚拟机提供安全访问控制服务。

虚拟防火墙允许用户通过自服务门户进行系统管理及访问控制规则（ACL）的配置，从 IP 地址、端口、协议等多个维度对流量进行检测和控制。通过配置 ACL 规则，用户可以自如地控制不同网络之间的互访流量，细粒度的进行安全隔离以及流量控制。

5.2.3.4 弹性负载均衡（ELB）

1、服务定义

弹性负载均衡服务（Elastic Load Balance）将硬件负

载均衡器虚拟出多个虚拟负载均衡器，VDC 业务员将云主机关联到负载均衡器，负载均衡器根据用户设定的负载均衡策略，将业务请求均匀分发到与之关联的云主机上，使得各个云主机的业务负载均衡，保证业务的稳定性和可靠性。

2、服务要求

提供弹性负载均衡实例服务，根据设定的负载均衡策略，将业务请求均匀分发到与之关联的云主机上，使得各个云主机的业务负载均衡，保证业务的稳定性和可靠性。

用户指定 VPC 管理 ELB 的指定名称、描述、Provider、VIP、绑定的 EIP。在已创建的 ELB 上管理监听器，包括名称、描述、负载均衡协议及端口、负载均衡算法、会话保持等，并同时创建健康检查。

用户为监听器配置健康检查，用于检查后端云主机的运行状态，包括健康检查协议、检查周期、超时时间、最大轮询次数等，与监听器创建合一。将后端云服务器/物理机添加到指定的监听器后面，设置 Member 的权重。

5.2.3.5 弹性 IP 服务（EIP）

1、服务定义

弹性 IP 地址是一个静态外部 IP 地址，将弹性 IP 地址和云主机相关联。通过弹性 IP，用户可从 Intenet 访问虚拟机。

当所关联虚拟机故障或需要升级时，可以迅速将弹性 IP

地址重新映射到另一个正常工作的备用虚拟机，无需变更虚拟机客户端的配置继续从备用虚拟机获得服务，从而降低业务影响。

实现云分区私网与公网的互通，保证客户业务访问入口不变。用户对已经申请的弹性 IP，可以执行以下操作:

（1）绑定弹性 IP 地址

将申请到的弹性 IP 地址和路由网络中关联的虚拟机进行绑定，使虚拟机可以通过固定的公网 IP 地址进行公网访问。

弹性 IP 所在的 VPC 和虚拟机接入网络所在的 VPC 相同。

（2）解绑定弹性 IP 地址

如果虚拟机不再提供公网服务，或者在公网服务地址不变的情况下更换业务虚拟机时，可以解绑定弹性 IP 地址。

（3）删除弹性 IP 地址

删除不再使用的弹性 IP 地址。如果待删除的弹性 IP 地址已绑定虚拟机，须先解绑定，再删除。

（4）使用限制

方案中存在 SDN 控制器的情况下，才支持弹性 IP 服务的自动化配置。

此服务依赖于虚拟防火墙，无虚拟防火墙时无法使用。

2、服务要求

（1）支持从 Internet 访问虚机的目的 IP 地址转换;

支持从虚机访问 Internet 的源 IP 地址转换，可以从 Internet 访问 LB 的虚 IP。

（2）管理方面要求

管理方便，用户可以通过 web 页面或者开放 API，同时管理大量 EIP 实例。

（3）安全方面要求

完全控制，用户可以完全控制自己创建的 EIP 实例。

5.2.4 虚拟数据中心

1、服务定义

虚拟数据中心（Virtual Data Center），是将物理资源池化后，通过逻辑隔离技术基于业务需要灵活分配的逻辑数据中心，包括数据中心需要的计算、存储和网络资源（实现 DCaaS 服务），向最终用户提供一个虚拟的所见即所得的数据中心。

2.服务要求

（1）灵活匹配组织结构：VDC 划分方式可以灵活多样，可以按照场景要求划分。

◎可以按部门划分，每个部门可以独立管理本部门资源，VDC 间互相隔离。

◎可以按使用领域划分，例如：开发 VDC，测试 VDC 等。

（2）VDC 资源配额：可以设置每个 VDC 的资源使用配额（包括 CPU，内存，存储，网络），VDC 资源配额可计量，成

本可视化。

（3）VDC 资源构建，支持跨多个物理数据中心，支持资源的统一分配。

VDC 自运营和自运维，每个 VDC 是一个具有自运营和自运维能力的独立管理实体。在 VDC 内，用户可以自助申请、管理及监控 IT 资源。

5.2.5 硬件托管服务

1、服务定义

IDC 托管服务即主机托管服务（服务器托管服务）或机房机柜服务，是指用户拥有自己的服务器，并把它放置在 Internet 数据中心的高标准机房环境中,并通过高速数据端口接入互联网。由客户自己进行维护，或者是由其它的签约人进行远程维护。由 IDC 机房提供具有通信电源，并可存放一定数量服务器的标准机柜给用户，且具有配套的网络资源，如出口带宽等。

2、服务要求

一个标准机柜功率为 4KW 以上，采用双路交流供电。

（1）云数据中心 1U 机柜空间：机柜总高度为 42U，配备柜顶交换机。

（2）云数据中心 2U 机柜空间：机柜总高度为 42U，配备柜顶交换机。

（3）云数据中心 1 个机柜空间：机柜总高度为 42U，配

备柜顶交换机。

5.3 技术要求

5.3.1 组网要求

5.3.1.1 整体组网要求

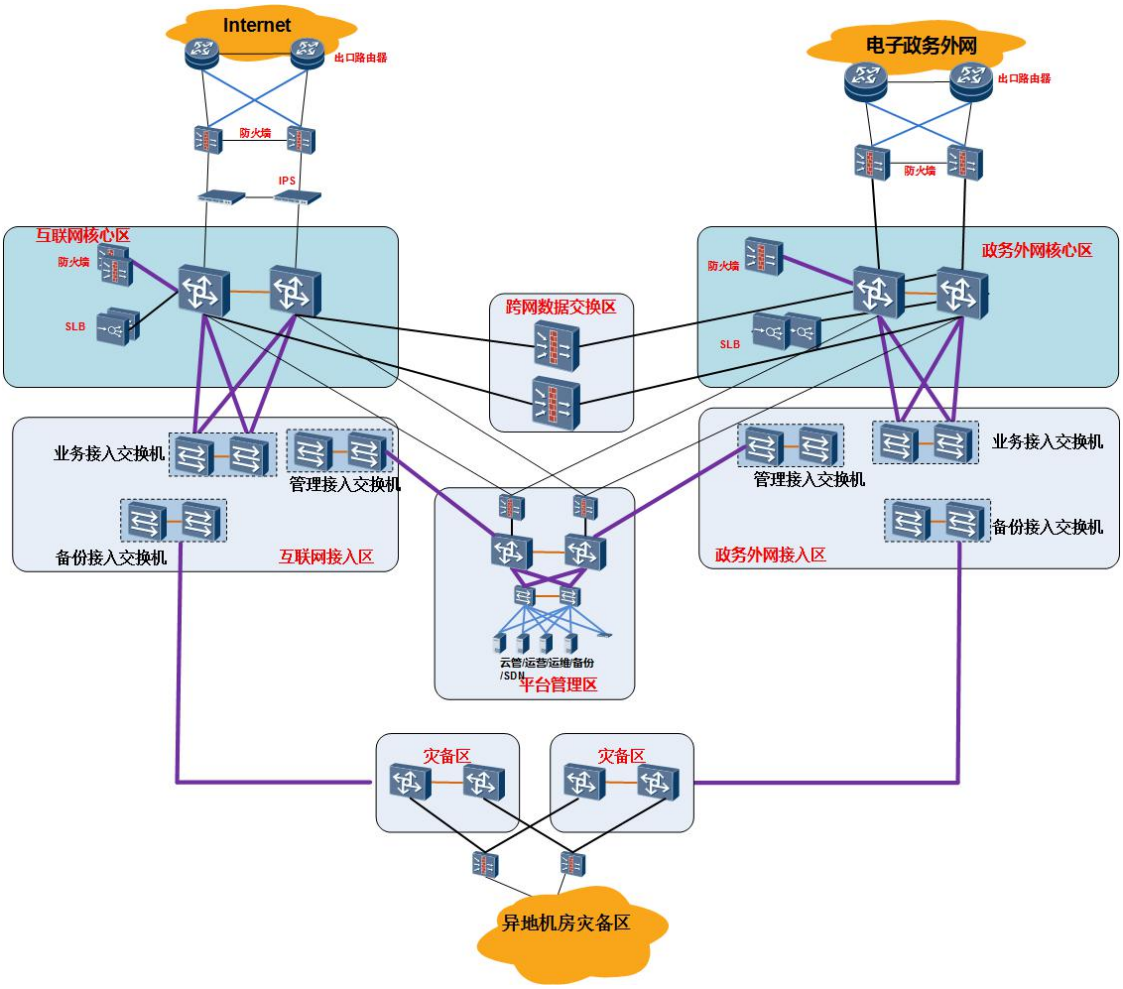
总体上，平台采用“云网协同”的网络设计方案，通过SDN实现租户网络的动态创建和维护。为每个委办局创建不同VPC网络，满足不同的业务上云的需求。核心和接入交换机启用VxLAN功能，实现委办局在数据中心内的安全隔离。各委办局通过政务外网接入数据中心，进行计算、网络、存储资源的访问。

数据中心网络部署采用基于SDN+VxLAN的部署方案,SDN控制器提供业务自动部署功能、控制器自动下发配置及自动化运维，VxLAN实现跨二层虚拟机迁移及多租户隔离。

政务云数据中心的网络设计采用“分区+分平面”原则。

根据业务系统情况将数据中心内网络划分互联网区、政务外网区、管理区、安全数据交换区以及异地灾备区。互联网区和政务外网区强逻辑物理隔离，两个区域需要数据交换时，通过网闸或者防火墙组成的安全数据交换区来进行。

在数据中心内部将网络划分管理、业务、存储三个平面，三个网络平面物理相互隔离，互不影响。服务器通过不同网卡接入不同网络平面。

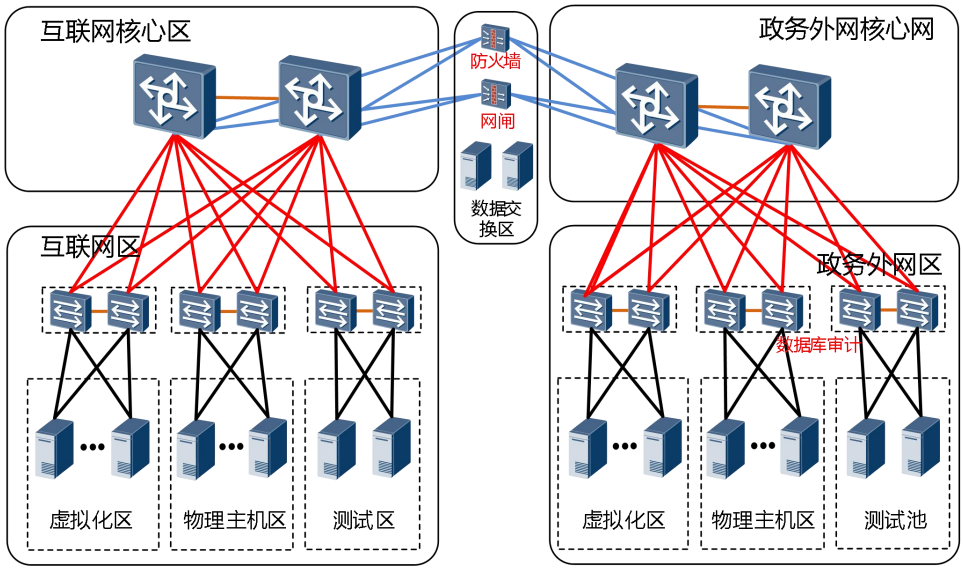


5.3.1.2 数据交换区网络建设要求

在政务外网区与互联网区之间，部署防火墙/安全隔离网闸，实现了对数据内容严格过滤和摆渡交换。通过安全数据交换区的数据交换系统，既从物理上隔离、阻断了具有潜在攻击可能的一切连接，又进行了强制内容检测，有效地在两网之间实现安全隔离与业务数据安全、可靠交换，从而实现最高级别的安全。

互联网核心区、政务外网核心区分别直接从核心区的核心交换机与数据交换区的防火墙/网闸相连，完成政务外网

与互联网区的安全、可控的数据交换。避免互联网业务受到攻击时，影响外网区核心业务区的业务和数据安全。



5.3.1.3 管理区网络建设要求

政务云数据中心内部所有主机、管理数据中心内部所有主机、服务器、网络设备、存储设备都会通过带内管理网口、带外网口分别上联到带内管理交换机、带外管理交换机上。通过带内网管对数据中心内服务器、存储、网络设备等进行管理；服务器带外管理，可以提供远程唤醒服务、作为带内管理的补充手段。

管理区根据功能可以分为以下区域：

1、网络核心区

部署边界防火墙和交换机，以保证管理区的安全。服务器带内管理口上连到带内管理接入交换机，而服务器、存储、网络、安全设备的带外管理口均接入到带外管理交换机；带内管理接入交换机和带外管理接入交换机统一接入到管理

核心交换机；管理功能区和管理操作区通过管理接入交换机接入到管理核心交换机上；此外在数据中心内，管理核心交换机连接到业务核心交换机,实现业务网络的统一 SDN 编排。

2、管理功能区

提供管理及安全服务器的部署，包含：OpenStack 的管理服务器、网管平台、SDN 控制器，以及堡垒机、安全认证、安全审计、漏洞扫描等安全设备。

3、管理操作区

与其他区域管理隔离，为管理人员、IT 人员提供管理接入能力。

5.3.2 软件要求

5.3.2.1 新建平台

采用基于 OpenStack 框架的虚拟化平台和 IaaS 层分布式数据中心管理平台。

所有新建平台必须采用与省级平台相同的 IaaS 层云平台软件。

所有新建的应用系统和迁移上云的应用系统需部署在新建平台之上。

项目	参考指标
基本	国产自主品牌，非 OEM 产品，具有国产软件自主知识产权
管理规格	支持管理≥300 个 Region
	支持管理≥1000 个虚拟数据中心（VDC）
	单个可用区（AZ）支持≥10000 台虚拟机

	支持定义≥5 级审批流程，每级审批支持≥10 个用户审批
	单 OpenStack 支持≥10000 台虚拟机
服务规格	单台虚拟机支持≥255vCPU，≥4T 内存，≥16 块网卡，≥10 块磁盘
	单个计算节点支持上电的虚拟机≥100 台
	单个计算节点支持≥2048 块虚拟磁盘
	单个计算节点支持≥2048 块虚拟网卡
	每个云磁盘支持挂载给≥16 个云主机/物理机，支持创建≥32 个快照
	单个 VDC 支持≥30000 个卷，≥60000 个卷快照
	支持虚拟机设备直通，可将 GPU、SSD 等直接映射给虚拟机使用
	支持物理机服务，用户可登陆直接申请物理机，并由系统自动完成服务器 OS 安装、网络配置和外围存储 LUN 的创建挂载等。
	支持虚拟机弹性伸缩服务，用户可以自助配置业务系统在特定的时间或者按固定的周期，或者根据业务系统的业务压力自动的增加或者删除业务系统内的虚拟机
	支持共享镜像服务和私有镜像服务
	支持备份服务化，用户可以通过管理平台申请对自己的部分或全部虚拟机或者虚拟机的磁盘做备份，用户可以自行设置备份策略。
	支持虚拟机高可用服务。用户可以通过管理平台申请对部分或全部虚拟机提供跨数据中心的 HA 能力，可以通过跨数据中心的存储双活。
	支持云硬盘高可用服务。用户可以通过管理平台申请针对自己部分虚拟机的磁盘提供双活保护
	支持服务自定义。管理员可以灵活的定义已有服务，支持用户可申请服务的白名单能力。

5.3.2.2 已建平台改造

对于符合《广东省“数字政府”政务云管理办法》及相关文件规定，允许继续留存运转的已建政务云平台，需要进行必要的改造，以统一纳入省级平台统一管理。已建平台不允许扩容和升级。

5.3.3 硬件要求

5.3.3.1 计算设备

5.3.3.1.1 ECS 服务器

项目	参考指标
基本	国产品牌，非 OEM 产品
CPU	≥2 路 10 核，主频 2.40GHz，或同等性能配置
内存	≥512G
存储	≥2 块 900G SAS 硬盘，或同等容量配置
接口	≥2 张双口 16G HBA 卡，≥3 块双口万兆网卡
扩展	支持≥24 个内存插槽
其它	长期工作环境温度支持 5-45 度
	使用国产管理芯片

5.3.3.1.2 BMS 服务器

5.3.3.1.2.1 物理服务器 I 类

项目	参考指标
基本	国产品牌，非 OEM 产品
CPU	≥4 路 16 核，主频 2.10GHz，或同等性能配置
内存	≥512G
存储	≥2 块 900G SAS 硬盘，或同等容量配置
接口	≥2 张双口 16G HBA 卡，≥2 块双口万兆网卡
扩展	支持≥9 个 PCI-E 插槽
其它	支持≥48 个内存插槽
	使用国产管理芯片

5.3.3.1.2.2 物理服务器 II 类

项目	参考指标
基本	国产品牌，非 OEM 产品
CPU	2 路 10 核，主频 2.20GHz，或同等性能配置

内存	≥256G
存储	2 块 900G SAS 硬盘，或同等容量配置
接口	2 张双口 16G HBA 卡，4 块双口万兆网卡
扩展	支持≥24 个内存插槽
其它	长期工作环境温度支持 5-45 度
	使用国产管理芯片

5.3.3.2 存储设备

5.3.3.2.1 集中式存储设备

5.3.3.2.1.1 普通 IO 存储设备（SAS/NL-SAS）

项目	参考指标
基本	国产品牌，非 OEM 产品
控制器	控制器≥4 个，任意 3 个控制器/3 个缓存板故障均不影响业务。 每控制器缓存≥512G，整机最大支持≥8T 缓存（不含任何性能加速模块或 NAS 网关缓存、FlashCache、PAM 卡，SSD Cache 等）。
接口	≥16 个 16G SFP+接口
磁盘	根据业务模型配置 SSD、SAS、NL-SAS 硬盘
特性	启用分级存储、快照、拷贝、克隆、卷镜像、自动精简配置、QoS、多租户、数据销毁、多路径、数据迁移等功能
架构	多控全交换式架构，控制器之间（SAN 和 NAS）采用高带宽、低时延的 PCI-E、Rapid-IO 或 IB 高速总线互联方式，非 FC、IP 协议或者 FC、IP 接口互联;
接口类型	支持 FC（8G、16G）、iSCSI（1G、10G）、FcoE（10G）、IB（56G），以及智能 IO 卡（4 口，支持 8/16Gb FC、10GE 和 FCoE）
RAID	支持 RAID 1、RAID3、RAID 10、RAID50、RAID 5、RAID6 等
容量	最大支持 3200 块磁盘。
其它	磁盘、电源、IO 模块都可以不停机热插拔
	有功能全面，图形化的管理软件，包括：盘阵，卷管理软件。配置存储的图形化管理配置和监控软件。

5.3.3.2.1.2 高 IO 存储设备（SSD）

项目	参考指标
基本	国产品牌，非 OEM 产品
控制器	控制器≥4 个 每控制器缓存≥512G，整机最大支持≥8T 缓存（不含任何性能加速模块、FlashCache、PAM 卡，SSD Cache、NVRAM 等）
接口	≥16 个 16G SFP+接口
磁盘	根据业务模型配置适合数量的 SSD 硬盘
特性	启用 LUN 智能数据重删压缩使用许可
架构	原生全闪存架构。双控之间 A-A，多控 scale-out 扩展架构，可扩展为≥16 个控制器，控制器之间采用高速 PCIe 或者 IB 连接。
时延	稳定时延≤0.5ms
重删压缩	提供全局在线重删和压缩技术，非后重删和压缩技术；在线重删和在线压缩支持均可单独开启或者关闭
细粒度块管理	应用感知的全闪存架构，可按照业务类型设置基础块大小，以实现细粒度的 SSD 块读写，IO 大小（Size）支持 4K/8KB/16K/32K，块粒度大小可调整。
重定向写	系统全部采用重定向写的方式，非传统硬盘的覆盖写方式
接口类型	支持 FC（8G、16G、32G）、iSCSI（10G、25G、40G、100G）、FcoE（10G）、IB（56G），以及智能 IO 卡（4 口，支持 8/16/32G FC、10/25G iSCSI 和 FCoE）
RAID	RAID5、RAID6、RAID-TP（容忍 3 盘同时失效）
容量	最大支持 2400 块磁盘。
其它	支持≥8192 台主机，≥16384 个 LUN
	兼容 AIX，HP-UX，Solaris，Linux，Windows 等操作系统
	支持中标麒麟、银河麒麟、凝思磐石等主流国产操作系统
	支持达梦、南大通用、人大金仓等主流国产数据库产品

5.3.3.2.2 分布式存储设备

项目	参考指标
品牌	国产品牌，非 OEM 产品，拥有自主知识产权，非开源软件开发，如不能使用开源 Lustre 和 Ceph 软件等。
分布式架构	基于全分布式架构的存储软件，支持构筑在 x86 服务器或 ARM 架构服务的硬件之上，通过软件层面的全分布式架构和数据冗余技术，来达到高可伸缩性和高可用性；性能、容量随节点数增加而线性增加。
	产品支持分布式块存储、文件存储和对象存储协议能力；支持部署分布式块存储/文件存储/对象存储/块存储和文件存储/块存储和对象存储/文件存储和对象存储/同时部署块、文件和对象存储，要求不同存储类型创建不同物理池，支持物理集群统一管理。
	存储服务器节点部署分布式存储软件组成分布式存储池，计算服务器至少可以以 SCSI、iSCSI、NFS、CIFS、HDFS、S3/Swift 等访问分布式存储池。
	块存储支持卷信息查询、在线扩容、卷拷贝、快照、精简配置、链接克隆等功能； 文件存储支持配额、快照、WORM、异步复制等功能； 对象存储支持对象重删、话单、同步复制等功能。
系统扩展性	扩容时支持不停机情况下的数据自动迁移和均衡。
	单集群可支持扩展至≥4000 个节点，单一系统支持 PB 级存储容量。
	单一系统存储容量可扩展至≥100PB
系统缓存	支持资源池内 SSD Cache 加速特性：每个资源池支持采用 SSD 介质提供写缓存、预读、读热点三种 Cache 能力。缓存空间自身必须具备容错和掉电数据保护机制，缓存介质故障或断电时，保证缓存中数据仍可恢复；无掉电保护功能的内存不允许作为写缓存使用。依赖 RAID 卡形式的 Cache 能力不满足需求。
系统部署要求	块存储可支持：10GE 以太网/RoCE、25GE RoCE、56Gb/s IB 组网，支持 RDMA 访问协议 文件存储支持：10GE RoCE、56Gb/s IB 组网，支持 RDMA 访问协议

	对象存储支持：10GE RoCE、56Gb/s IB 组网，支持 RDMA 访问协议
	组网全冗余部署，无单点故障。
	支持单套分布式存储系统上同时混合承载虚拟化（桌面云、服务器虚拟化等）和非虚拟化（数据库物理部署等）业务数据存储场景。
协议要求	可支持 SCSI、iSCSI；兼容 OpenStack Cinder
资源池管理要求	可支持按服务器维度划分多个存储资源池；支持图形化界面划分存储资源池；每个存储资源池即为一个故障域；至少支持存储资源池间卷的离线迁移；支持后台数据恢复或再平衡等任务的 IO 流控。
	分布式存储系统支持通过 Portal 创建存储池，创建时可以支持选择主存、缓存、副本数、安全级别，可选择服务器进行创建 。
数据保护	支持 2 副本或 3 副本数据冗余模式，满足不同可靠性要求的业务场景，本次配置 3 副本。
iSCSI 特性	支持 iSCSI CHAP 认证，防止 iSCSI Initiator 和 iSCSI Target 之间未经授权的非法访问
快照	支持卷快照功能(Snapshot),单个卷支持的最大快照数量不少于 60000 个，相比无快照情况下卷读写性能无下降。
兼容性	支持 KVM 虚拟化平台，支持对接 OpenStack，提供 cinder driver，支持 cinder-volume 标准接口。
	分布式块存储提供的客户端应该支持 SuSE、RedHat、Oracle Linux 等通用的 Linux 系统。
卷规格	单系统支持存储卷的数量不少于 1000000 个。
	单卷最大容量支持≥256TB。
性能要求	Cache 命中 70%场景下，单 PB 有效容量系统下单卷 8K 随机读写比 7:3，IOPS 应不低于 10 万。
	单 PB 有效容量系统下单卷 1M 顺序读写比 7:3，带宽应不低于 1500MB。
	Cache 命中 70%场景下，单 PB 有效容量系统下全系统 8K 随机读写比 7:3，IOPS 应不低于 120 万。
	单 PB 有效容量系统下全系统 1M 顺序写总带宽应不低于 15GB。

可靠性	必须支持读修复管理：即在读数据失败时，如果是磁盘扇区读取错误，系统会自动从其他节点保存的副本读取数据，然后重新写入该副本数据到硬盘扇区错误的节点，从而保证数据副本总数不减少和副本间的数据一致性
远程容灾保护	1、提供具备全分布式存储 A-A 双活架构，双活站点单系统最大可扩展超过 100 存储节点。 2、提供双活架构，实现两套核心存储数据双活（主机能够并发读写同一双活卷），任何一套设备宕机均不影响上层业务系统运行。 3、双活架构支持独立的第三方仲裁，第三方仲裁设备故障时，不影响业务运行，同时双活卷仍能保持数据实时一致；同时，可支持优先站点仲裁。 4、提供基于卷和虚拟机两种粒度配置双活，实现双活服务化。
硬件管理要求	支持磁盘亚健康管理功能：支持定期检测磁盘 SMART 信息，判断磁盘亚健康情况（硬盘扇区重映射数超过门限、读错误率统计超标、慢盘），并在磁盘损坏前进行隔离并告警。
	支持网络亚健康管理功能：支持针对存储节点的网络出现丢包、错包、延时大、速率不匹配等故障现象可提供故障告警并自动尝试修复。
	支持存储节点亚健康功能：如果存储节点在由硬件或者软件故障导致处理速度慢于其他节点时，分布式存储软件可以自动检测对应的节点，发出告警并提供处理方案。
	支持磁盘漫游功能，同一存储节点内支持任意个存储磁盘交换位置，以防止维护时的误操作。
系统管理要求	支持对块存储系统的 CPU 利用率、内存利用率、带宽、IOPS、时延、磁盘利用率、存储池利用率等的统计。
	支持通过 SNMP 协议向第三方平台上报告警。

5.3.3.3 网络设备

5.3.3.3.1 SDN 控制器

项目	参考指标

架构开放性	控制器架构需要具备高度的开放性，支持 MD-SAL 组件开发平台，复用 ONOS 和 ODL 两大开源控制器的优秀成果，快速提高控制器的功能完备度和商用可靠性，持续受益于开源控制器社区的技术演进。
多种 Fabric 组网兼容	支持通过一套完整的 SDN 控制器支持多种 Fabric 场景的能力，灵活满足不同场景的方案部署诉求，支持的 Fabric 网络包括：Network Overlay 集中式网关组网、Network Overlay 分布式网关组网以及 Hybrid Overlay 分布式网关组网。
运维管理能力要求	支持通过 SNMP 协议自动发现网络设备，并添加至控制器； 支持通过 LLDP、LLTD 多种链路发现协议发现网络设备之间、网络设备与主机之间的链路。对 VxLAN 网络中可能存在的环路现象，控制器可以检测出网络中的环路故障点，并提供给管理员破除环路的手段。支持检测的环路类型有单设备单端口环路、单设备多端口环路、跨设备环路多种。
可靠性能力要求	计算节点双归接入到两台 ToR 设备，且这两台 ToR 需配置唯一的虚拟 VTEP IP。建议使用 iStack 或者 M-Lag 技术配置虚拟 VTEP IP，实现流量一致性。
裸金属网络发放	支持与云平台上的裸金属机管理组件协同，自动下发裸金属机业务部署所需的网络配置。
标准业务链	支持 IETF 标准的安全服务链模型，采用 PBR 或 NSH 作为引流技术，引导业务流量到不同的服务节点上进行相关业务处理，实现拓扑无关的、图形化编排的、自动配置的业务链功能。业务链上所能提供的增值服务应包括 Firewall、NAT、IPSec VPN 以及 Load Balance。
云网数据一致性	当与云平台数据不一致时，支持全量和增量同步，避免配置冲突。

二次编排	对接云平台的场景下，云平台上的业务配置并不一定能完全满足用户需要，需要控制器能够还原云平台上的逻辑网络业务，并赋予用户再次编辑的能力，为用户提供更完整的业务能力。

5.3.3.3.2 核心交换机设备

项目	参考指标
整机规格	包转发率≥172000Mpps，业务插槽数量≥8，独立的交换网槽位数≥5，支持 N+1 冗余。
系统架构	Clos 架构、信元交换，主控引擎与交换网板硬件分离,支持独立的 1+1 监控板实现监控面和管理通道分离。
风扇及散热	风扇框冗余设计，要求可独立拔插的风扇框个数≥3。 任意风扇框故障或者不在位不能造成业务中断。 任意风扇框可独立拆卸和维护，要求严格前后风道设计，保障散热效果，避免机柜左右间的级联加热。 线卡前面板开孔进风，加快光模块散热，延长光模块寿命。
虚拟化技术	支持多虚一技术堆叠技术，可实现跨机箱的以太网链路捆绑和单一界面管理整个多机箱的交换机;支持带外管理方式进行集群或堆叠部署，主控板上提供专用 GE 端口用于集群或堆叠协议报文传送。
数据中心特性	支持 IETF 标准的 VxLAN、NSH 协议，满足数据中心 SDN 网络要求，产品均采用智能自研芯片，通过标准 NSH 协议的业务编排，以便满足此次设计方案中对安全业务流量的自动编排,使得业务功能与网络解耦,安全更加灵活部署。
可靠性	网络核心设备提供双主控、双风扇槽位冗余、电源冗余配置，所有业务板卡及电源、风扇模块均可热插拔。

5.3.3.3.3 业务接入交换机设备

项目	参考指标
整机规格	10GE 光口≥48，40GE 光口≥6，40G 多模光模块≥4，万兆多模光模块≥40，双电源模块，风扇框 2 个。
风道	支持前后、后前风道。

接口缓存	缓存≥12M。
虚拟化	支持堆叠，堆叠带宽≥240G，堆叠系统中设备数量最大可支持16台。
数据中心特性	支持IETF标准的VxLAN、NSH协议，满足数据中心SDN网络要求，产品均采用智能自研芯片，通过标准NSH协议的业务编排，以便满足此次设计方案中对安全业务流量的自动编排，使得业务功能与网络解耦，安全更加灵活部署。

5.3.3.3.4 带外接入交换机设备

项目	参考指标
整机规格	GE电口≥48，10GE光口≥4，40GE光口≥2，万兆多模光模块≥2，双电源模块，风扇框2个。
风道	支持前后、后前风道。
接口缓存	缓存≥8M。

5.3.3.4 安全设备

5.3.3.4.1 核心防火墙设备

项目	参考指标
硬件架构	采用多核架构，双主控，双电源，接口板和业务板分离，电源、主控板、接口板、业务板支持热插拔，支持40G，100G接口，便于平滑扩展需要。
性能要求	吞吐量≥40Gbps,最大并发连接数≥4000万,每秒新建连接数≥50万，最大虚拟防火墙数≥2000。
路由能力	支持静态路由、路由策略、策略路由、RIP、OSPF、BGP、ISIS等路由协议，支持IPv6协议栈、IPV6穿越技术、IPV6路由协议。
智能选路	支持基于链路最小延时、带宽、权重比例的多出口智能选路，支持基于应用的智能选路。
业务	支持深度业务识别，并对识别出的流量进行带宽限制。

识别和流量控制	
负载均衡	支持服务器负载均衡功能，其负载均衡算法包括但不限于简单轮询、加权轮询、最小连接、加权最小连接等，支持智能 DNS，设备与 DNS 服务器配合，不同 ISP 的用户 DNS 请求可以得到不同的 IP 地址。
入侵防御	支持基于漏洞的入侵防御技术，基于漏洞的入侵攻击特征库数量≥2300 种；支持用户自定义入侵防御签名。

5.3.3.4.2 出口防火墙设备

项目	参考指标
配置要求	配置双主控，双电源，万兆光口≥6，千兆光口≥24；IPSec VPN 隧道≥95；吞吐量≥40Gbps，最大并发连接≥3900 万；配置应用层协议识别及流量控制功能，3 年应用协议特征库升级；配置负载均衡功能；配置 IPS 防护吞吐量≥20Gbps，防病毒吞吐量≥16Gbps。
硬件架构	采用多核路由器架构，双主控，双电源；除两个主控板外，整机扩展插槽≥3；接口板和业务板分离，电源、主控板、接口板、业务板支持热插拔。
性能要求	配置吞吐量≥40Gbps，最大并发连接数≥4000 万，每秒新建连接数≥90 万，最大虚拟防火墙数≥2000。
路由能力	支持静态路由、路由策略、策略路由、RIP、OSPF、BGP、ISIS 等路由协议，支持 IPv6 协议栈、IPV6 穿越技术、IPV6 路由协议。
智能选路	支持基于链路最小延时、带宽、权重比例的多出口智能选路，支持基于应用的智能选路。
业务识别和流量控制	支持深度业务识别，并对识别出的流量进行带宽限制。

负载均衡	支持服务器负载均衡功能，其负载均衡算法包括但不限于简单轮询、加权轮询、最小连接、加权最小连接等，支持智能 DNS，设备与 DNS 服务器配合，不同 ISP 的用户 DNS 请求可以得到不同的 IP 地址。
入侵防御	支持基于漏洞的入侵防御技术，基于漏洞的入侵攻击特征库数量≥2300 种；支持用户自定义入侵防御签名。

6 PaaS 平台建设要求

6.1 总体要求

6.1.1 技术路线要求

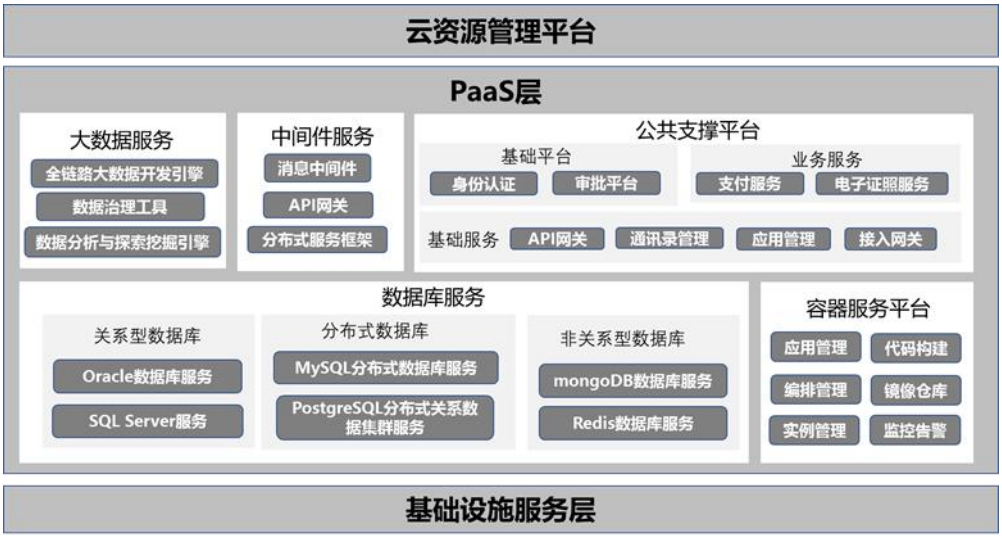
PaaS 平台的建设应满足“统一访问、动态调度、弹性伸缩”的要求，应提供数据库、中间件、大数据套件、容器等服务能力，为各部门构建健壮、灵活的基础信息架构，做到“集中部署、各取所需、灵活应变、简化维护”。各部门除了可以直接在 PaaS 平台上搭建应用系统外，还可以根据具体需求，调用 PaaS 平台的应用接口，因地制宜地进行二次开发和集成，构建本部门的信息系统实体。

数据库服务需支持主流的数据库引擎，并对底层数据库引擎统一封装，以公共的数据访问接口，提供面向多租户的统一数据库访问服务及数据库服务水平扩展能力；中间件服务主要提供消息中间件、API 网关以及分布式服务框架等云化中间件服务，并以统一接口的形式提供给用户进行服务调用；大数据服务主要提供数据集成、计算框架、配置管理、信息加工工具、可视化管理工具等大数据应用所需的基础能力。

6.1.2 总体架构

政务云 PaaS 层，需要建设统一管理、统一服务的平台服务。地市各部门用户作为政务云平台服务的使用者，应在不需要购买数据库和开发软件的情况下，直接使用 PaaS 平台的服务，快速地建立自己的信息系统。

根据“数字政府”政务云平台建设总体架构，地市 PaaS 层架构图如下:



1、数据库即服务提供对底层数据库的统一封装，提供公共的数据访问接口，提供数据库资源池和数据库水平扩展能力，支持分布式数据库，支持数据库本身的多租户管理。

2、中间件服务主要提供应用中间件服务和消息中间件服务等，中间件服务建设重点是搭建中间件资源池，形成可以管理和调度的资源和单元。

3、政务云平台的 PaaS 平台提供大数据套件服务，实现数据提取、处理、分析、报表展示、客户画像、机器学习等大数据功能，满足“数字政府”政务云平台的大数据处理需

求。

4、容器服务主要提供以容器为核心的、高度可扩展的高性能容器管理服务，解决用户开发、测试及运维过程的环境一致性问题，并以统一接口的形式提供给用户进行服务调用。

5、公共支撑平台为用户提供协同办公的基础性支撑平台，各类信息化应用提供功能完整、性能优良、可靠性高的技术公共组件。

6、PaaS 层还将结合云管平台完成 PaaS 层面资源管理功能的建设。

6.2 服务要求

6.2.1 数据库服务要求

数据库服务要实现统一建设、统一管理、统一服务，数据库资源可以随着硬件资源的扩展而扩展，满足业务量增长的需求。各地市单位根据不同的数据库应用场景选择合适的数据库，政务云平台提供关系型数据库、非关系型数据库以及分布式数据库三种类型的数据库。

6.2.2 中间件服务要求

中间件是基础软件的一大类，属于可复用的软件范畴。中间件在操作系统软件、网络和数据库之上，应用软件之下，总体作用是为处于上层的应用软件提供运行的开发环境，帮助用户灵活、高效的开发和集成复杂的应用软件。

主要提供的中间件服务为：消息中间件服务、分布式服务框架以及 API 网关。服务提供由云管平台集成中间件自动交付功能，通过可视化界面选择对应的中间件类型、环境配置等，实现中间件环境的自动交付构建。

1、消息中间件服务

消息中间件用于存储进程间传输的消息，为分布式部署的不同应用之间或者一个应用的不同组件之间提供基于消息的可靠的异步通信服务。

2、分布式服务框架

分布式服务框架是一个围绕应用和微服务的平台，提供全生命周期管理能力和数据化运营支持服务，提供与应用、服务、机器有关的多维度监控数据，助力服务性能优化。分布式服务框架基于 Spring Cloud，支持分布式服务发布与注册、服务调用、服务鉴权、服务降级、服务限流、配置管理、调用链跟踪等功能。

3、API 网关

API 网关是 API 托管服务，提供 API 的完整生命周期管理，包括创建、维护、发布、运行、下线等。API 网关可使用 API Gateway 封装自身业务，将用户数据、业务逻辑或功能安全可靠的开放出来，实现自身系统集成以及业务连接。

6.2.3 大数据套件服务要求

大数据套件服务基于开源 Hadoop 生态和自研组件，对

外提供可靠、安全、易用的大数据套件。用户可按需部署大数据套件以实现数据提取、处理、分析、报表展示、客户画像、机器学习等大数据应用功能。大数据处理套件的具体服务要求如下:

1、大数据开发引擎

提供拖拽式的可视化数据开发 IDE，为大数据集成、存储、计算环节提供多渠道数据集成、多类型存储支持、离线批处理计算、实时流处理计算、可视化工作流开发 IDE、文本检索及检索分析等大数据开发能力。

2、数据分析与探索挖掘引擎

提供数据分析、探索、挖掘一体化大数据能力，包含基于纬度建模的多维分析、交互式探索分析、机器学习、深度学习、可视化敏捷报表门户等功能，向用户提供强大的数据分析与数据挖掘能力，助力大数据的价值发现。

3、数据治理工具

提供数据元信息管理功能，支持字段级别的数据权限管控，包含库表数据字典、数据血缘跟踪与溯源、热点数据分析等特色功能，以提高海量数据资产的管理效率。

6.2.4 容器服务要求

政务云平台容器服务提供从 code 到 cloud 的一站式能力，覆盖开发、测试、构建、部署、运维等所有环节，可以简化环境的部署，改变应用的交付模式。容器服务可以让用

户像使用一台超级计算机一样使用整个集群，有效降低资源管理门槛。同时自动化的作业调度、资源保证和隔离，可以让多业务共享集群，提升资源使用率，保证伸缩性和可靠性。

具体服务要求如下:

1、应用管理

对应用的生命周期管理，在满足不同的应用属性基础上，实现 Stack、app、instance 的创建、删除等基础操作，以及应用的升级或回退、应用弹性伸缩、应用健康检查等功能。

2、编排管理

提供编排模板可视化、查看关系图、YAML 编码和操作记录等功能，并可通过编排模板作为入口对模板进行部署编排。

3、实例管理

提供实例版本升级、实例停止使用、通过 Webshell 直接在网页进入实例内部等功能。

4、代码构建

代码仓库收到新的提交代码可以自动触发单元测试，并对通过测试的、新的镜像同步到镜像仓库，以便后续选择镜像快速部署创建应用。

5、镜像仓库

提供镜像仓库，根据需求镜像可分为个人镜像、业务镜像、公共镜像等，提供基于不同角色的权限管理、镜像自动化构建、常用镜像统计、镜像自动安全扫描、镜像同步等功

能。

6、监控告警

提供实例、应用、业务、节点等各种资源对象指标展示、设置指标阈值、监控集群的健康状况进行异常事件告警等功能。

6.2.5 公共支撑服务要求

公共支撑服务面向政府民生和协同办公等各类信息化应用，提供功能完整、性能优良、可靠性高的技术公共组件，解决应用系统建设中的共性问题，实现低成本快速地构建应用。公共支撑服务基于完全开放的技术路线，实现对现有基础技术设施进行兼容，同时支持扩展各种优秀的技术组件和框架，以构建完备的公共技术支撑体系。公共支撑服务的公共组件经过长时间、高并发、复杂环境的检验，成熟度高，可快速投入到应用系统构建中。

6.3 技术要求

6.3.1 数据库技术要求

政务云提供的数据库，具体要求包括但不仅限于以下内容:

1、支持并行操作所需的技术，包括多 CPU 并行和多服务器并行、事务处理的完整性控制技术等。

2、支持可按需定制计算节点及存储节点数量。

3、从数据库服务层面上，必须至少提供MySQL、oracle、MongoDB、redis以及PostgreSQL等数据库引擎服务，并且要将数据库作为一种服务，能够实现多种类型数据库的即开即用、弹性扩展。

4、从数据库用户使用层面上，支持提供用户自服务门户和API接口，可自行创建不同规格的数据库实例，并提供数据库实例的扩容、自定义备份、数据恢复、性能监测分析、异常告警、日志管理等功能。数据库性能要求具备高可用性，采用全冗余架构，无单点故障。每个关系型数据库实例均实现主从热备，平均可用性不低于99.99%。

5、从数据库统计层面上，支持按照不同空间实现对应用的统计、应用健康状态对应用的统计、CPU、内存、磁盘数进行应用统计。

6.3.2 中间件技术要求

6.3.2.1 分布式服务框架建设要求

分布式服务框架具体要求包括但不仅限于以下内容:

1、全面的分布式服务

分布式服务框架: 基于Spring Cloud，支持分布式服务发布与注册、服务调用、服务鉴权、服务降级、服务限流、配置管理、调用链跟踪等功能。

Dubbo客户端平滑迁移: 对于已经在使用 Dubbo 框架的用户，通过修改 pom.xml 中的依赖，支持非常平滑地迁移

到分布式服务框架。

2、应用全生命周期管理

资源管理：分布式服务框架实例支持添加云服务器，物理服务器及 Docker 容器作为分布式服务框架中的设备资源，同时可进行分组管理。

应用基本管理和运维：在分布式服务框架控制台上，支持一站式完成应用生命周期的管理，包括创建、部署、启动、停止，也支持扩容、缩容操作。

3、立体化监控

IaaS 基础监控：监控服务器资源的磁盘 IO、内存、CPU、网络等指标，以监控图标形式展示，精准掌控服务器健康状况。

调用链跟踪：服务间可能存在较长的调用链条，通过调用链跟踪，在控制台上会呈现出可视化的调用链关系，可以发现耗时较长或者出现异常的服务。

监控告警：支持设置自定义告警阈值，当指标触发告警条件时，会发送及时的告警信息，预防突发情况。

6.3.2.2 消息中间件建设要求

消息中间件具体要求包括但不仅限于以下内容：

1、消息处理

支持万级 Topic，支持百亿级别消息堆积、单 Queue 性能超过 5000QPS，队列数可弹性扩展，同时具备消息回放、

即时投递、消息匹配、消息过滤等功能，对于不符合标准的消息应进行校验和拒绝。

2、集群管理

支持集群部署与主备自动切换技术，集群规模自动扩缩和集群横向扩容时，支持对用户透明。

3、服务保障

在海量堆积的情况下，应始终保持高性能，不影响集群的正常服务，同时提供流量控制功能，保证服务可靠性。

4、监控管理

支持集中化的自身监控和可视化的 Web 管理界面，支持消息服务管理，显示消息队列中状态，同时具备主备手动、自动切换技术。

5、其他要求

支持多种客户端语言，如 Java、Python 等主流客户端语言,提供 JAVA/Python/C/C++/.NET 多 SDK 接入。同时基于 paxos、raft 等强一致性算法，提供多副本存储，提供实时、强一致落盘能力，以及同城跨机房、双活部署能力。

6.3.2.3 API 网关

API 网关具体要求包括但不仅限于以下内容:

1、生命周期管理

支持 API 的创建，配置，修改，测试，上线，运行和下线的完整生命周期管理功能，同时针对 API 发布，提供测试、

预发布和发布三种环境，可随时回滚指定环境到特定版本。

2、配置管理

支持 API 网关用户直接在管理控制台进行图形化配置，支持调用 API 进行配置，同时支持用户根据自身业务对 API 服务进行流量配置。

3、端口管理

对外提供 HTTP / HTTPS / HTTP & HTTPS 的 API 接口，后端可对接 HTTP / HTTPS / SCF/微服务等不同的后端业务，统一对这些后端业务进行管理。

4、监控管理

支持实时监控 API 调用情况，提供多维度视角，用于流量分析，错误分析，并支持秒级请求过滤和控制，同时支持可视化的监控界面，用户可在 API 网关上直观的管理 API 的使用情况。

5、其他要求

支持自动生成符合 Swagger 规范的 API 文档与 SDK 的功能，便于提供给调用者使用。

6.3.3 大数据套件技术要求

政务云大数据套件建设具体要求包括但不仅限于以下内容:

1、大数据开发引擎

（1）实时数据接入

支持 Flume、Kafka\hippo 数据接入，包含结构化、半结构化、非结构化的数据秒级实时接入。

（2）离线数据导入

支持 MySQL、Postgre、Oracle 等主流关系数据库高效导入，支持文本类日志数据离线导入。

（3）支持多类型存储

支持分布式文件、对象存储、NoSQL 从 GB 到 PB 量级的存储，满足复杂存储应用场景。

（4）可扩展要求

高可扩展设计，存储系统可动态随数据量增加从 G 到 P 级的动态扩容，支持系统不停机动态扩容。

（5）离线批处理计算

支持 MapReduce、Hive 批处理计算作业，可支撑数仓建设中的数据清洗、转换、汇集、主题提取等数据处理需求。

支持 Spark 分布式内存计算框架，在内存中对数据集进行快速的多次迭代，以支持复杂的数据挖掘算法和图计算算法。

（6）实时流处理计算

支持基于 Spark 上的 Spark Streaming，满足毫秒级的实时计算场景需求，如实时推荐、用户行为分析等。

（7）可视化工作流开发 IDE

支持拖拽式的工作流开发 IDE，简单 Web 式拖拽操作来

完成整个大数据工作流的任务开发。

2、数据分析与探索挖掘引擎

（1）多维分析引擎

基于 Apache Kylin 开源分布式分析引擎，为用户提供基于 Hbase 存储的数据 Cube 预建模及百亿行规模的 SQL 数据分析能力，满足用户面向部门的数据集市建设需求。

（2）交互式数据探索

采用列存储技术、万维标签查询处理技术，提供实时的多维交互式 SQL 查询、统计、分析系统，支撑万级维度、千亿级规模下的秒级数据统计分析需求，支持数据离线导入及在线数据实时接入。

（3）分布式数据库

支持 SQL 2003 核心扩展的分布式关系数据库，完全兼容 PostgreSQL 的 SQL 语法，支持主键、触发器、约束、函数、存储过程、跨节点 join 等绝大部分的 SQL 特性，同时满足百 T 级数据规模的 OLTP 和 OLAP 应用场景。

内核级支持数据库分库分表，分库分表逻辑对业务完全透明化，简化业务的数据访问逻辑。

内核级支持冷热数据分治，业务无需感知底层存储介质的差异，对外提供一个统一的数据库视图，可有效降低服务器硬件成本。

（4）机器学习

集成 Spark、Python、R、XGBoost 等 4 种机器学习框架，支持图计算和深度学习，内置分类、回归、聚类、关联规则等 60 余种丰富算法。

可视化的 Web 拖拽式任务流开发，能够让算法工程师和数据科学家从数据和模型的角度以最自然的流方式来思考，充分激活大数据活力。

支持机器学习任务的团队协作开发，提高数据探索发现效率，有效助力知识沉淀与共享。

3、数据治理工具

（1）数据权限管控

提供对关系数据库、分布式数据库、HDFS 文件、Hive 库和 Hbase 的文件、库、表、字段级的数据权限控制能力，满足用户在不同场景下对不同粒度数据的安全管控能力。

实时记录敏感数据访问行为以支持定期的安全审计，支持自定义敏感数据访问预警策略，严控内部数据安全风险。

（2）数据字典

可视化 Web 式元信息管理工具，满足用户对海量数据的元信息检索、标注、数据口径标准化等诉求。让用户能高效的对数据资产进行管理、索引、查找，有效提高数据资产管理效率。

（3）血缘分析、直系分析和重要性分析

提供血缘分析、直系分析、重要性分析等数据治理工具。

元数据分析可直观了解到数据的来源、数据之间的关系、数据与任务的计算关系、数据流向、数据被引用次数等重要信息，便于用户直观的把握数据资产状况。

6.3.4 容器技术要求

PaaS 平台的容器服务建设要求包括但不限于以下要求:

1、支持兼容 kubernetes 全能力，适配 IaaS 的基本能力。提供基于 kubernetes 开放的 CBS、CLB 等，支持多种开源应用一键部署到容器集群中，提升部署效率。

2、容器服务支持在服务器实例中启动，独享计算资源，集群运行在私有网络，支持自定义安全组和网络 ACL。

3、支持分布式服务架构，实现服务故障自动修复、数据快速迁移；结合有状态服务后端的分布式存储，实现高可用服务和数据的安全。

4、无需使用集群管理软件和设计容错集群架构，简化大规模集群管理和分布式应用的管理、运维。支持启动容器集群，并指定想要运行的任务，即可完成所有的集群管理工作。

5、实现镜像极速下载和上传，海量容器秒级启动，提高容器部署效率；可以对提交的业务代码进行快速构建、测试和打包集成，将集成的代码部署到预发布环境和现网环境上。

6、支持灵活集群托管，安排长期运行的应用程序和批

量作业。集成负载均衡，支持在多个容器之间分配流量，自动恢复运行状况不佳的容器，保证容器数量满足需求。

6.3.5 公共支撑技术要求

公共支撑服务包括但不仅限于以下部分:

1、支持基础支撑，提供准入网关和 API 网关。

2、支持应用支撑，提供包括应用管理、容器服务、微服务框架、工作流引擎、表单引擎、消息队列、分布式事务引擎等功能。

3、支持业务支撑，提供包括统一身份认证服务、电子证照服务、事项服务、电子支付服务、物流服务、电子印章服务、电子签章服务、电子归档服务等功能。

6.4 接口要求

地市 PaaS 开放对接要求主要是为了满足云管平台统一管理、统一运维的需求，以及用户基于 PaaS 进行二次开发的需求，实现对地市应用基础资源的管控和利用。地市云 PaaS 提供开放接口，让云管平台管理 PaaS 层拥有的各种资源、采集资源的有关数据，以及集成第三方的运维平台。同时，用户也可以利用开放接口，根据业务需要进行定制和个性化开发。

PaaS 能力的开放场景主要包括资源管理能力开放、监控能力开放、二次开发能力开放。

1、资源管理能力开放

为了让用户可以通过云管平台自助快速地进行数据库、消息中间件等 PaaS 资源的申请、详情查看、管理、销毁等操作，PaaS 层需要提供相应的开放接口，与云管平台对接。

2、监控能力开放

云管平台需要完成服务器、网络设备等监控数据的采集和存储，为用户提供预警，日志查询、报表统计、性能服务指标比对等功能。因此 PaaS 层需要提供开放的监控接口，与云管平台对接，让其完成数据的采集。

3、运维能力开放

为了让用户可以通过云管平台直接对 PaaS 层的资源进行全生命周期的运维管理，实现运维的集中化、可视化和自动化，PaaS 层需要提供相应的开放接口，与云管平台对接。

4、二次开发能力开放

用户可以通过调用 PaaS 层的接口，进行二次开发，主要是消息中间件接口（队列接口、消息接口、主题接口、订阅接口等）以及 API 网关的接口等。

7 SaaS 平台建设要求

7.1 总体要求

7.1.1 技术路线要求

建设可共用、可复用的 SaaS 云服务。政务云 SaaS 层，在 IaaS 层提供的基础设施资源上，依托 PaaS 层服务部署一些通用的公共应用，为全市各单位提供按需使用的软件服务，

使各部门不再需要自建和运维相应的应用系统，避免重复建设。

通过统一建设云公共应用服务可以减少或取消全市各单位购买、构建和维护基础设施和应用程序次数，只要需申请政务云平台的资源，即可快速获得统一即时通讯服务、智能图像服务、视频服务等公共应用服务。将应用软件部署在统一的资源池上。

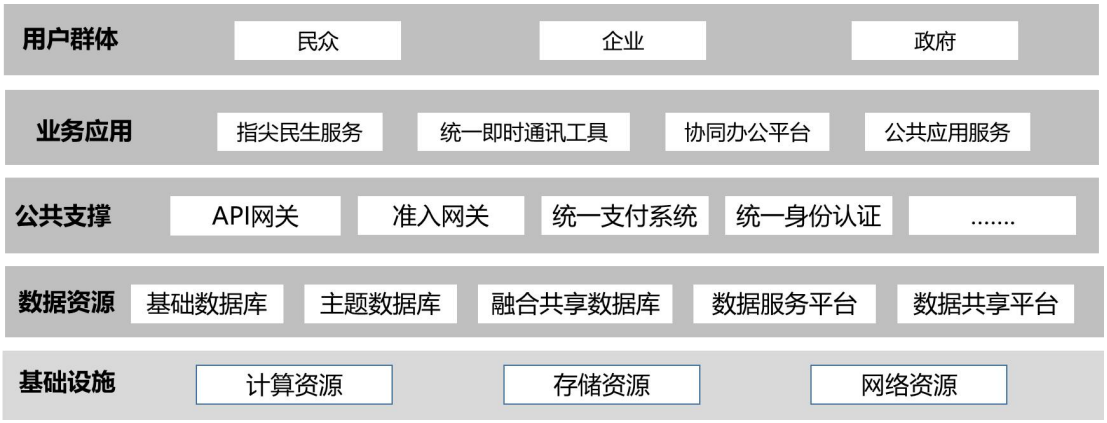
从应用角度上，SaaS 所有应用必须满足对申请使用本应用的租户进行弹性的资源分配，提供支持多个租户的应用模式，各租户间进行租户隔离，这些资源的分配和租户的管理，要求支持由云管平台统一资源调度与管理，对 SaaS 应用资源和租户进行接管。SaaS 层可以在租户和资源管理上，进行线程级别的监控，将各 SaaS 应用上的各模块的运行状态、性能指标等进行统一的管控。

从基础设施角度上，SaaS 层应用在 IaaS 层提供的基础设施资源上依托 PaaS 层服务，进行自动化部署。全市各单位租户在云服务门户申请 SaaS 层应用服务，由云管平台下发服务申请，IaaS 层和 PaaS 层自动分配所需资源，完成应用部署。

7.1.2 总体架构

基于政务云 IaaS 层提供计算资源、存储资源、网络资源，PaaS 层提供公共支撑组件和数据资源，SaaS 平台为全

市各单位提供可共用、可复用的 SaaS 云服务，主要包括：指尖民生服务、统一即时通讯工具、协同办公平台、智能图像服务、智能客服等 SaaS 服务。



7.2 服务要求

7.2.1 协同办公平台要求

建设 SaaS 化协同办公平台，支持软件即服务的服务模式，各单位可低成本获得协同办公系统软件服务，实现低成本运维，“零编码”个性化定制。可通过组件化配置或少量代码实现 OA 系统核心功能开发，降低二次开发和维护要求、节省开发周期，提高财政资金投资效益。

协同办公服务平台建立移动政务应用体系， 建设涵盖公文处理、协同办公、系统管理、信息发布系统、文档管理、档案管理等功能的集约化 OA 平台，实现政府部门内部和跨部门跨层级的办文、办公、行政管理的信息自动化。

协同办公工作台利用政务微信的即时通讯能力让用户实现随时随地跨越部门边界的沟通，并通过数据接口汇聚事务性工作，供用户集中处理，简化操作，提高工作效率。

7.2.2 指尖民生服务要求

各地市可基于PaaS层提供的公共支撑、微服务架构以及容器服务，快速部署指尖民生服务，实现“一门式一网式”民生服务，各部门不再需要自建和运维相应的应用系统，避免重复建设,并且可以利用政务云IaaS和PaaS能力，集成微信刷脸、实名认证、非税支付、车牌OCR识别、拍证件照等API，向用户提供指尖服务。

将各个业务系统以WEB（http、https）方式开放办理接口，接入到智能网关，统一接入，统一监控。统一UI设计和前端开发，统一界面，以用户体验为目标，通过前台集中，进一步带动后台整合，促进流程简化，推行网上政务协同，让群众感受到在线服务的便利，实现“一门式一网式”民生服务。

1、民生服务微信小程序

在小程序里面应一站式办理所有政务民生服务。以小程序为移动端主入口，辅以PC端网上办事大厅，汇聚民生服务办事能力，各部门业务办理系统以安全方式对民生服务后台支撑开放接口。提供办理接口管理工具，监控业务接口运行和质量情况，供各部门各地市作为管理抓手进行督办，提高民生服务质量。

2、民生服务微信公众号

通过微信公众号，推送各类证件到期提示，服务办结通

知，服务评议，投诉应答等消息，群众查看消息可以快速链接到服务办事入口，通过指尖触达，建立和用户的快速连接。

3、民生服务后台支撑

提供业务应用接入规范、流程，对各局委办的已有业务系统、对新建设的系统接口 API 进行快速集成，为小程序提供业务调用接口，从而实现服务事项在小程序中快速上线、提供服务。

7.2.3 统一即时通讯工具要求

统一即时通讯服务是针对融合办公业务需求而为客户协同办公能力，助力客户信息化建设，实现语音、视频、即时通信、数据等多种通信功能的有效集成，为市级各单位提供功能丰富、融合便捷的沟通环境，实现及时、高效的通信。

统一即时通讯服务由客户端、开放平台、基础框架、运营管理、办公协作等几个核心模块组成，平台的部署支持单个和多个数据中心的部署。

1、客户端

统一即时通讯服务提供面向不同终端平台的标准版本的客户端版本，覆盖了 Windows、Mac、Android、iOS 等用户最常用的操作系统。为了支持广东省各省级单位应用的各类个性化需求，提供完善的客户端扩展框架，第三方的开发商可以基于该框架对客户端进行二次开发。

2、开放平台

统一即时通讯服务开放平台提供即时通讯能力和企业级应用的整合能力进行封装，形成统一的 OpenAPI，对外提供标准化的开放服务。

3、基础框架

统一即时通讯服务基础框架包含即时通讯平台最核心的能力，包括对于基础 IM 沟通、高级 IM 沟通、复杂组织架构、安全管控的核心框架的支持能力。

4、运营管理

统一即时通讯服务作为一个高频使用的基础信息化平台，为了最大化的发挥其价值，必须充分保障其稳定、高效的运行。运营管理模块提供一系列运营保障能力，包括完整的多级授权体系、系统管理和监控能力、新旧版本升级对接能力。

5、办公协作

基于统一即时通讯服务所提供的各个模块，可以与各省级单位内部的各个办公系统、业务系统进行对接，实现全方位的办公协作，从而提升信息化对日常业务运作的支撑能力。

7.2.4 政务服务网要求

各地市可基于 PaaS 层提供的公共支撑（统一身份认证、电子证照服务、统一申办、统一待办等）、微服务架构以及容器服务，快速构建政务服务网，提供全流程一体化在线服务。通过智能网关与各支撑应用服务交互，纵向整合政府服

务、决策保障、跨域协作等服务域应用，横向汇聚省政府各个直属部门的专业应用，为办事群众和企业提供一个风格统一、方便智能的一网式政务服务办事渠道，主要包括个人事项、法人事项、政务公开、政民互动、便民利企等功能。

7.2.5 公共应用服务要求

需求无需开发自建，直接使用 SaaS 平台的公共应用，包括但不限于智能图像服务、视频服务智能客服务服舆情分析服务云盘服务短信通知服务位置服务以及辅助决策支持方法库字典管理、模型管理、模型分类管理、模型信息查询、模型库匹配管理、模型调试管理等，提供 ETL 工具对数据源进行抽取转换和联机分析处理工具，迅速构建各种类型所需的数据分析报告和领导驾驶舱，同时提供完整的 BI 展现功能，支持集成数据展现、安全管理等应用。

8 云管平台建设要求

8.1 总体要求

8.1.1 技术路线要求

建设一套逻辑上统一的云管平台，符合“数字政府”政务云平台要求的“统筹管控平台+资源子服务平台”两级建设架构，一方面在资源层面实现无缝管理，另一方面在业务层面实现业务服务统筹运营。

对于政务云平台，通过统一云资源管理平台，在资源层面实现无缝管理；在业务层面实现统一管理，包括资源、账号的开通、控制、预警；在运营层面实现分级管理，云平台及其下层基础软、硬件资源由云运营单位负责运营管理，云平台用户单位对其所属资源的分配、管理具备最高权限，只有在用户单位确认委托或授权的情况下，政务云运营单位才能对用户的业务资源进行管理；扩展层面通过标准的接口体系，实现第三方平台接入纳管。

8.1.2 云管平台总体架构

按照“1+N+M”的“数字政府”政务云平台总体框架，建设各地市的“一朵云”，并纳入省级政务云统一管理，支撑跨层级、跨部门的数据共享和业务协同，云管理平台的建设应实现以下目标:

1、提供统一的云资源管理服务，实现云资源统一管理。

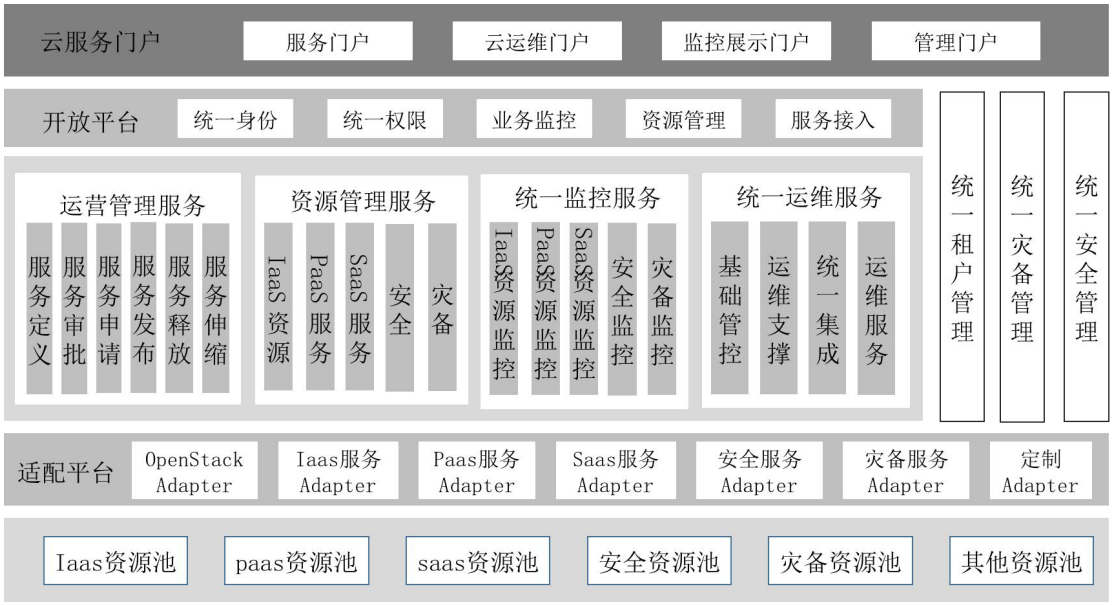
2、资源层面，实现无缝管理。

3、业务层面，实现统一管理。资源和账号的开通，资源控制、监控和预警都是在资源管理服务中统一的无差异化管理。

4、扩展层面，实现接口管理。建设统一的云资源管理接口体系，实现标准的资源监管 API、流程工单 API、资源计量计费 API 等。未来政务云平台的新增云服务通过与统一云管标准 API 对接，实现新的云服务上线。市级已建政务云

平台通过与标准的资源监管 API 对接，实现统一监管。

具体的云管理平台架构如下图所示:



8.1.2.1 服务要求

1、云服务门户

云管平台面向不同的角色提供相应的服务门户，以便进行云服务的申请、云平台的运维、资源的监控和用户权限的管理。

2、开放平台

开放平台主要是将各种云管理的基础能力通过 API 的方式统一对外提供，此外还需提供业务监控接入能力、统一身份认证能力、统一权限管理能力、服务接入能力。

3、运营管理服务

提供一套逻辑上统一的云管平台，一方面在资源层面实现统一管控，包括计算资源、存储资源、网络资源、数据库资源、中间件资源、安全资源、备份资源等云资源。另一方

面，在业务层面实现业务服务统筹运营，即实现云资源申请、资源变更无差异化管理。

4、资源管理服务

资源管理定位于底层基础子服务系统与上层业务管理平台之间，一方面支持多种子服务平台管理接口，实现对资源统一分配和管理，另一方面对上层业务应用提供标准的管理接口，做到无差别兼容管理。

5、统一监控服务

建设“采集层，存储层，业务层，接口层”四级监控体系，对云平台的资源使用和服务能力进行整体监控。

资源使用监控。以基础云的资源数据为基础，监控云平台资源现状，如计算资源的数量及使用率、存储资源的容量及网络资源的使用情况等。

服务能力监控。对云服务的各项关键指标进行综合分析，快速了解云平台服务提供情况。

6、统一运维服务

统一运维平台对云平台 IT 资源进行运维管理，依托 SOA 设计理念将运维平台以基础管控层、运维支撑层、统一集成层、运维服务层输出服务，提供各层资源全生命周期的运维管理，实现对 IT 资源的集中化、可视化、自动化管理。

7、统一租户管理

云管平台可以根据各部门的组织层级，按照实际使用场

景，划分不同的租户，各组织层级可灵活的关联到基础云的不同租户，满足资源隔离的目的。对云平台的各个租户，根据权限的不同，集中管理身份认证信息、授权信息、配置信息等，实现资源的有效共享与合理分配。

8、统一灾备服务

对接各个灾备系统，为云平台提供业务应用同城和异地的灾备部署、备份恢复、容灾演练和灾备切换等服务，保障业务数据的一致性、完整性和可恢复性。

9、统一安全服务

云管平台统一安全服务以服务为导向，提供给租户的安全服务包括两方面的内容：整体的基础安全服务和有针对性的租户安全服务。

基础安全服务。为保障云平台整体安全所提供的安全防护，包括网络边界防护、虚拟机隔离等平台基础安全防护内容

租户安全服务。租户安全服务为云平台提供给租户的安全能力，租户根据自身业务情况，可以选择相应的安全服务内容，并自行配置相关的安全策略。

10、统一适配平台

保证不同体系和架构的云安全接入云管平台，实现统一管控、差异屏蔽，为上层应用管控云资源提供统一 API 能力。

8.1.2.2 技术要求

1、云管平台高可用要求

（1）基础云平台本身支持容灾架构，任意云管理控制器宕机，云平台也能正常运行，正在创建的虚拟机也能继续创建完成。

（2）云平台中无单独的共享存储设备（SAN 和 NAS）时，当虚拟机所在物理服务器发生故障时，能够自动在其它物理服务器重新启动虚拟机，尽快恢复业务的运行。

（3）云平台网络控制器支持分布式部署架构，在任意管理控制节点出现故障时，云平台网络仍然能够正常工作，不影响业务运行。

（4）云平台存储控制器支持冗余架构，任一存储控制器出现宕机故障时，不影响云存储业务的运行；同时，云存储数据切片冗余保存多份，存储节点出现故障时，数据不丢失且不影响上层业务正常运行。

2、易用性要求

（1）操作界面要充分考虑操作易用性，适合运维人员日常操作习惯，为用户提供图形化向导界面。

（2）必须提供完善易用的 RESTful API 接口及文档，对云内所有资源及功能（如：主机、硬盘、网络、负载均衡器、防火墙、弹性 IP、监控等）提供 API 级别的支持。

（3）支持云内资源的网络拓扑图展示功能，直观展现网络结构。

3、PaaS 功能支持

（1）云管支持 PaaS 服务能力，提供集成的关系型数据库提升开发与测试效率。

（2）提供高性能的关系型数据库服务，支持 MySQL、MSSQL 等多重数据库引擎，提供包括单机部署、主从部署或高可用架构等各种管理功能。

（3）提供金融级分布式关系型数据库服务，兼容 MySQL 协议语法，具备多种类型的分区支持，分布式的架构可支持平行扩展、性能与容量线性增长。

（4）提供云化 Oracle 功能，支持单机、高可用等多种部署模式，优化过的存储集群、计算集群为 Oracle 应用提供卓越的 TPM/IOPS 性能。

4、SaaS 功能支持

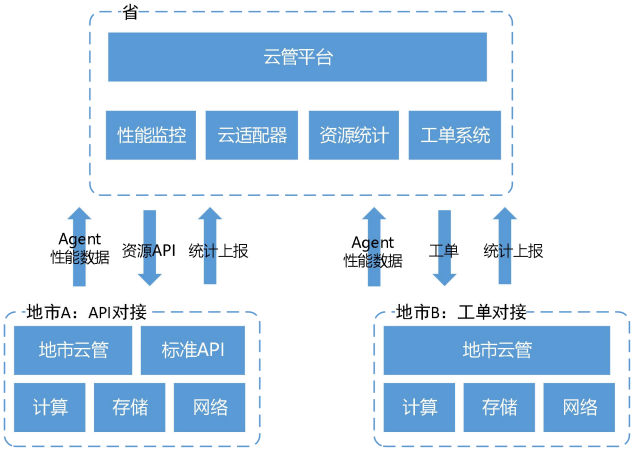
（1）云管平台支持 SaaS 服务能力，通过接入多种 SaaS 生态服务，提升平台整体的应用效率。

（2）提供 SaaS 源码管理平台服务，支持在本地管理源代码版本库，支持实时异地备份。

8.1.3 省与地市云管平台架构

建设统一的云管平台，作为“全省一片云”架构的“数字政府”政务云平台的统一资源管理平台，新建地市级云平台原则上都需要接入全省统一的云管平台。各地市也可根据实际需求建设地市级云管平台。省级云管平台与各地市级云

平台的对接架构如下图所示：



省市对接符合以下统一管理的目标：

1、统一的资源管理视图

从省云管能够统一管理各地市的资源，包括租户、用户、虚拟机、云存储等资源，包括资源的申请、管理和销毁，以及统一的审批流程。按照对接的级别，又分为 API 对接和工单对接，分别对应“云适配器”和“工单系统”。

云适配器：适配各地市的 API 接口，适配之后能够直接从省云管的接口直接下发和管理资源，要求地市的 IaaS 提供的接口符合省云管平台的要求。

工单系统：如果地市 IaaS 接口不能满足省云管的要求，那么可采用工单系统的方式对接，工单系统属于线上+线下结合的流程。

2、统一的性能数据视图

从省云管能够查看地市各 IaaS 资源的性能监控数据，地市的服务器（虚拟机+物理机）需安装云管性能数据采集 AGENT，以采集操作系统级别的性能数据、中间件数据，以

及采集客户业务自定义的数据，由省云管的“性能监控”模块进行数据处理，包括统一的告警配置、性能数据展示等。

3、统一的资源统计视图

从省云管平台能够查看各地市云的资源统计情况，各地市定期上报资源统计数据，包括计算、存储、网络等资源的使用量、剩余量等，然后由省云管平台的“资源统计”模块进行收集，并统一展示。

8.2 服务要求

云管平台需按照广东省政务云平台的云管平台建设技术架构建设，包括但不仅限于以下建设内容。

8.2.1 云服务门户

云服务门户主要包括云服务子门户、云运维子门户、云管理子门户和云监控子门户。云服务子门户主要是提供给各个云平台的用户使用，可通过该门户完成各种资源的申请和管理操作；云运维子门户主要是服务于运维管理人员，通过该门户实现对与运维管理有关的所有功能模块的操作；云监控子门户基于数据实时渲染等各种技术，实现云数据的图形可视化、场景化以及实时交互，让各级管理人员、用户更加方便地进行数据的个性化管理与使用。云管理子门户主要服务于运营管理组织及人员，通过该门户实现对所有运营管理功能模块的操作。

8.2.2 资源管理服务

云管平台可根据访问量自动伸缩应用所占的计算、存储、网络带宽等资源，对计算、存储、负载均衡、网络等资源的使用做到精细化管理并提供统计分析功能。同时，云管平台需要确保云平台的资源可以虚拟化、弹性扩容和灵活调度，以及运行在虚拟机上的服务高度可用。

8.2.3 运营管理服务

运营管理服务从资源管理系统中调取所有云资源及服务，将资源及服务定义为不同类别、不同规格的云服务。最后将云服务发布到云服务目录中，供租户浏览和申请使用。

云管平台提供完整的服务生命周期管理，将云平台的计算、存储、网络、数据库、中间件、SaaS 应用、安全、备份资源以服务的形式提供给用户，用户可以从服务目录上申请。对于已经申请的服务，用户可以使用、维护、变更、释放。管理员可以定义服务、管理服务目录、审批用户提交的服务申请。

8.2.4 统一监控服务

云管平台可对服务器、网络设备等物理和虚拟资源的使用情况，以及服务的状态、用户的操作行为、触发的安全事件等进行统一监控。同时提供多渠道，多视图的监控告警，用户可以根据自己需要设定阀值并选择告警渠道。

8.2.5 统一运维服务

云管平台可对 IT 资源进行运维管理。依托 SOA 设计理

念，按照基础管控层、运维支撑层、统一集成层、运维服务层四个层次，提供各层资源全生命周期的运维管理，实现对IT资源的集中化、可视化、自动化管理。

1、基础管控层

基础管控层是上层运维服务体系与底层IaaS资源的连接器，为上层提供指令、文件、数据的通道，支持直连模式、代理模式以及为达到最优连接指定级联路由的模式。

2、运维支撑层

运维支撑层为基础管控层之上的管理与基础运维操作服务。

3、统一集成层

统一集成层是一个开放的平台层，包含用于支持用户简单快速地创建、部署和托管应用的PaaS服务，以及提供完善的前后台开发框架、服务总线（ESB）、调度引擎、公共组件等。

4、运维服务层

运维服务层是在PaaS之上快速构建的面向运维场景的解决方案的载体。它通过对底层各支撑模块能力的拼装，实现基础运维、CI/CD、监控告警、任务编排、弹性伸缩、安全审计以及移动运维等各类场景的自动化。

8.2.6 统一租户服务

通过统一租户管理服务对云管平台的各个租户、以及租

户下面的用户进行统一管理，并集中管理身份认证信息、授权信息、配置信息等。

根据各部门的组织层级，按照实际使用场景，划分不同的租户，各组织层级可灵活的关联到基础云的不同租户，满足资源隔离目的。

云平台的服务可以同时提供给多个租户使用；每个租户，有自己的云计算资源、云网络资源、云存储资源等；租户间使用的计算资源、存储资源、网络资源完全隔离，互不影响。

根据组织维度来进行云资源的管理和基于政府部门维度进行租户管理，实现与用户角色和权限体系的对接。

8.2.7 统一灾备服务

统一灾备服务，通过标准的接口体系，将全市分散的灾备系统纳入统一平台集约管理，通过统一门户提供全市集中的灾备服务的接入和运营管理，灾备资源和管理策略的统一纳管，面向服务化提供规范的灾备服务目录，实现现存和后续灾备系统资源和服务的接入。

平台面向全市提供多租户支持（用户及灾备资源隔离及计费）、资源监控管理、灾备策略配置管理、灾备作业管理、统计和报表管理、运维告警等服务。以标准化的云灾备服务模式向用户提供各种灾备服务目录和灾备 SLA 能力,让用户能够更安全快捷地使用。同时通过统一的管理视图,满足各种角色人员对灾备服务的管理需求。

8.2.8 统一安全服务

统一安全服务支持分租户管理，为多个租户提供个性化的安全能力，包括主机安全、WAF、漏洞扫描、态势感知等。同时集中进行系统安全监测，并为安全计算环境、安全区域边界、安全通信网络配置统一的安全策略。安全管理服务支持针对每个安全域的设备进行灵活的策略制定和管理，实现本安全域内的信息收集和处理。

8.2.9 统一适配平台

统一适配平台主要是为了保证各个云资源平台的安全接入，只有通过在统一适配平台进行注册的云资源平台才能接入到云管平台中，并向租户提供各类云服务。统一适配平台要能够支持多体系、多架构的不同云的接入，在满足对多云的统一管控、屏蔽差异的同时，为上层应用管控云资源提供统一的接口。

8.2.10 开放平台

开放平台主要是将各种基础支撑能力通过开放 API 的方式提供给外部使用，包括各种租户、IaaS 云资源、PaaS 资源等的管理 API，开放业务监控能力，业务方可以上报业务指标，由云管平台集中处理、存储和展示；开放统一身份认证能力，第三方系统可使用云管平台的统一认证；开放统一权限能力，第三方系统可以使用云管的授权体系；开放服务

接入能力，接入第三方的 PaaS、SaaS 服务。

8.3 技术要求

8.3.1 云服务门户

8.3.1.1 部门与用户管理

1、支持部门组织架构管理功能，能够新增、修改部门信息，支持设置部门管理员。

2、支持部门用户管理，管理员可定义用户的不同角色，通过角色管理来控制用户的权限。

3、提供子用户功能，管理员可对子用户进行管理，进行新建、修改、禁用、密码重置和删除等操作。

4、提供项目管理功能，支持将不同部门的用户按照项目组织在一起。

5、用户登录平台后，只能看到自己或团队权限范围内的云资源。

8.3.1.2 资源服务目录

1、提供云平台资源服务目录，服务目录需包含弹性计算、弹性存储、负载均衡、主流数据库常用云服务

2、支持平台管理员在服务目录中发布新的服务，或对已有的服务进行配置、删除处理等。

8.3.1.3 资源配额管理

支持为平台用户分配一定的资源配额，用户在配额范围

内可自助使用云平台的各种资源。

8.3.1.4 云资源使用与管理

1、平台支持接入多个独立的云资源池，支持使用同一套自助门户操作不同地域的云平台的资源和多云统一纳管。

2、支持云资源转交功能，管理员创建的云资源可转交给其他用户使用。

3、提供向导式资源操作界面，简化平台的操作难度。

4、提供在线帮助功能，提供平台常见操作和问题的知识库。

5、提供资源统计功能，支持按照部门或项目统计云资源的使用情况。

8.3.2 资源管理服务

8.3.2.1 资源虚拟化和扩容要求

资源虚拟化和扩容具体要求如下:

1、支持将物理服务器中的 CPU、内存、硬盘等资源抽象为可以统一分配和管理的逻辑资源。

2、支持业务量变化时资源可动态扩容。

3、支持自定义镜像和指定服务参数。

4、支持自定义 QOS 参数和不同 SLA 等级的虚拟机服务。

8.3.2.2 资源调度要求

资源调度具体要求如下:

1、支持手动或按策略调度虚拟服务器的资源，以及实

现虚拟服务器在不同物理服务器之间的迁移。

2、支持将多数据中心/资源池的资源进行统一管理和服务发放。

3、支持主流虚拟化系统的统一管理。

4、支持资源集中展现，查看各类资源的详情。

5、支持灵活定义 SLA 等级，以及根据需要在全局调度、分配资源。

8.3.2.3 高可用要求

高可用具体要求如下:

1、支持构建物理和虚拟服务器集群。

2、支持在虚拟服务器本身或者虚拟服务器所在物理服务器发生故障时，可以在集群进行故障切换。

3、支持虚拟服务器故障隔离，在一个虚拟服务器内发生的故障不会影响同一台物理服务器上的其它虚拟服务器和 Hypervisor。

8.3.2.4 虚拟机管理要求

虚拟机管理具体要求如下:

1、支持虚拟机常规信息的查看。

2、支持虚拟机的启动、暂停、停止、挂起、恢复、关闭等。

3、支持虚拟机的配置修改。

4、支持虚拟机远程 console 连接的管理。

5、支持虚拟机和模板的相互转换。

6、支持创建空白虚拟机以及从模板创建虚拟机。

7、支持对虚拟机的 CPU、内存、硬盘 I/O、网络流量使用情况的监控。

8、支持虚拟机任务、事件和告警日志的查看。

9、支持虚拟机迁移和虚拟机存储迁移。

8.3.2.5 按需能力订制要求

按需能力订制具体要求如下:

1、支持指定虚拟服务器可使用的 CPU、内存、I/O 等资源的最大值和最小值。

2、支持实际使用资源在运行过程中随工作负载在分配的资源范围内变动。

3、支持多个虚拟服务器的可使用资源大于物理服务器所能提供的资源，实现资源复用。

8.3.3 运营管理服务

8.3.3.1 服务定义要求

服务定义具体要求如下:

1、支持设置云平台提供的服务的名称、描述和图标。

2、支持设置用户申请服务时可以输入的服务参数。

3、支持设置管理员审批时可以配置的服务参数。

4、支持锁定服务参数，锁定的服务参数在用户申请服务时无法配置。

8.3.3.2 服务申请要求

服务申请要求至少包含以下内容:

1、可指定云主机的可用分区、操作系统类型、硬件规格、云主机所在网络，云主机个数。

2、可指定云存储的可用分区、硬件规格、存储类型、云磁盘个数。

3、可指定 VDC 的配额（CPU 核数、内存、存储、弹性 IP 个数、VPC 个数、安全组个数、虚拟机个数）、VDC 可使用的资源池。

4、可指定地域、VPC、弹性 IP 个数，以及硬件路由器的规格和公网 IP 池。

5、可指定物理机型号、操作系统、物理机个数。

8.3.3.3 服务审批要求

服务审批具体要求如下:

1、VDC 业务管理员可以审批来自 VDC 内用户提交的服务申请。

2、全局业务管理员可以审批来自 VDC 业务管理员提交的 VDC 服务申请。

（3）审批时，可以选择“同意”或“拒绝”，以及配置服务参数。

8.3.3.4 服务维护要求

服务维护要求至少包含以下内容:

1、支持云主机上/下电、重启、休眠、云主机转虚拟机模板、查看监控信息、创建云主机快照。

2、支持云存储挂载到云主机，或从云主机上卸载。

3、支持弹性 IP 绑定到云主机或负载均衡器，或从云主机、负载均衡器解绑定。

4、支持查看 VDC 配额使用情况和 VDC 下已申请资源列表，以及统计资源数量。

5、支持应用上/下电、修改应用、查看应用拓扑、具有弹性伸缩组的应用可根据应用负载弹性伸缩。

6、支持查看 VPC 网络拓扑和在 VPC 下管理网络、路由器、防火墙、安全组、弹性 IP、负载均衡器、VPN 等。

7、支持设置或修改监听器参数，包括协议类型（TCP、HTTP、HTTPS）、前端网络、后端网络、分配路由策略（轮询策略、最小连接模式）、最大会话数、健康检查信息（检查路径、超时时间、检查周期、最大重试次数、协议类型）等。

8、支持设置或修改定时备份策略、备份副本个数。

8.3.3.5 服务编排要求

服务编排具体要求如下:

1、支持根据模板规范自行创建编排模板，以及模板合法性检查。

2、支持根据编排模板创建各个资源，并生成资源唯一标识。

3、支持根据提供的编排模板和资源唯一标识，对原有编排模板中的资源进行修改。

4、支持查询资源标识列表和根据资源唯一标识查询资源信息。

5、支持通过资源唯一标识删除根据模板创建的所有资源。

6、支持根据资源唯一标识查询原有资源编排模板。

7、支持根据资源唯一标识查询资源的输出信息。

8.3.3.6 服务计量要求

服务计量具体要求如下:

1、支持按 VPC 的资源使用量进行业务结算，业务结算依据为 VPC 计量特性提供的计量数据，计量指标包括：CPU、内存、磁盘、弹性 IP、虚拟机个数、安全组个数、数据库服务节点数等。

2、支持实时查看每个服务实例的资源使用量计量。

8.3.4 统一监控服务

8.3.4.1 统一监控管理要求

1、提供定制化的大屏展示功能，动态展示云的资源及业务应用的统一监控告警情况，主要包括：云资源监控、资源容量、云服务运行状态监控、实时告警、设备统计、应用统计等。

2、支持日常运维所需的常用监控指标(包括 CPU、内存、

存储等)。如果用户需要某些下级管理系统支持但不常用的指标，需要能够提供定制能力，并可生成对应的报表。

3、支持对 WebLogic、Oracle、Apache、Tomcat、Nginx、SQL Server、HAProxy、Memcache、Redis、MySQL、RabbitMQ、Zookeeper 等常见组件的监控，同时支持用户开发接口，实现持续组件开发。

8.3.4.2 资源池管理要求

1、支持管理多资源池，对多个数据中心的资源集中管理，并支持按资源池－集群的关系查看每个资源池及资源池下的集群的资源情况及资源使用情况。

2、支持资源池权限管理，资源池管理支持分权管理，为各资源池指定管理员，且只能管理和查询其管理的资源池资源。

8.3.4.3 资源集中管理要求

1、支持资源集中化统一管理，管理的范围包括：物理服务器、存储设备、交换机、路由器等网络设备；虚拟机、存储卷、IP 网段的管理。

2、自动发现，支持云资产（虚拟机、存储、网络虚拟化资源）的主动识别、变更发现和主动修改。

3、支持通过 CMDB 配置管理统一管理各数据记录，包括应用系统及其运行环境中所有 IT 设备/系统及其配置信息得到有效完整的记录和维护，各 IT 设备/系统之间的物理和逻

辑关系。

4、支持通过 CMDB 配置资源间的关系，支持通过 CMDB 自定义扩展属性及父子节点关系等，有利于资产属性的扩展及关系的完善记录。

5、云平台自建 IP 管理系统，提供包括：全流程自动化的 IP 分配、回收，机房网络建设网络规划。

8.3.4.4 集中告警管理要求

1、支持多维度告警/事件展现。包括监控对象分类、物理位置、虚拟逻辑、来源系统、客户维度、自定义条件。

2、支持与外部监控系统的对接，支持多维度查看告警，包括活动告警、正在处理的告警、历史告警，可以查看告警详情、处理情况等信息。

3、支持查看选定告警的详情、告警源关联信息、关联对象告警、告警源详情、告警源性能。

4、支持告警自定义筛选。支持按多个维度的条件进行组合筛选，包括：资源池、告警级别、资源类型等相关条件。

5、支持性能阈值告警。当监控对象性能超过阈值时，自动产生告警，从而对数据中心设备性能及时产生预警。

6、支持告警后处理，系统支持邮件发送、短信发送和自动转事件处理流程等后处理操作。

8.3.4.5 服务管理流程要求

1、系统默认云运维常见流程，包括故障处理流程、问

题管理流程、服务请求流程、变更管理流程。

2、支持流程与自动化的整合，可以通过自动化的运维流程加速运维效率。

3、支持工作流程定制，提供的各项流程服务。

8.3.4.6 拓扑视图要求

1、支持从数据中心物理位置为维度层层钻取查看各资源间的拓扑关系，如机房到机柜、机柜关联的设备（物理服务器、存储设备、交换机、路由器等）、以及物理机上运行的虚拟机、虚拟机承载的业务系统。

2、支持拓扑对象操作、支持拓扑对象查找、支持大屏展示。

3、支持通过拓扑图查看各资源间的关联关系。

4、提供云平台虚拟与物理资源统一动态视图，可在此视图中了解物理设备与虚拟资源之间的关系（例如查看物理机上运行的所有虚拟机及其信息），并且提供搜索、查找、定位的能力，且视图数据由云平台自动生成，无需手工导入。

8.3.4.7 业务监控要求

具备对各类业务监控进行接入的能力，包括对用户业务所在服务器运行状态的监控，服务进程监控，业务特性监控以及业务拓扑展示，可将整个业务的逻辑拓扑进行直观展示以及实时监控以及业务指标的趋势查询。

8.3.4.8 资源计量及统计分析报表要求

1、统计报表，支持统计平台中所包含的物理机资源、虚拟机、存储资源、网络资源等资源信息；统计各类资源的用户使用量、每类资源的使用情况，如基础云平台、业务系统的 CPU、内存、存储、IP 的资源总量及占用量。

2、支持云报分析，按月统计各资源池资源容量情况、资源开通情况、以及资源使用率情况等，并支持报表导出。

3、支持周期性生成报表，周期类型包括：天、周、月、季度。只需要设置一次报表参数，即可周期提供报表数据。

8.3.4.9 监控总览要求

1、应提供平台的资源使用和服务能力总览，为用户了解平台运营情况提供快速入口。

2、支持实时展示平台的资源现状，如计算资源的数量及使用率、存储资源的容量及网络资源的使用情况等。

3、支持对云服务的各项关键指标综合分析，根据服务能力进行不同的颜色展示。

8.3.4.10 监控中心要求

1、提供“告警中心+工单管理”的一体化集成监控中心，运维人员通过监控中心可以对云资源的异常告警通过工单的方式进行及时处理和管理。

2、支持云平台所有资源的异常告警展示，运维人员可在对告警工单进行认领并处理。用户可设置告警查询的条件

（如业务模块、服务器 IP 等）。

8.3.4.11 性能服务监控要求

1、支持多种方式对云计算资源的性能数据进行采集，用户可设置相关的条件对其进行多角度、深层次、更清晰地监控，包括 CPU、磁盘和内存等。

2、支持云计算环境的性能监控，及时发现和排查问题，合理调配资源，进行科学的规划及部署，确保云计算资源的合理运行。

3、支持平台服务能力集中监控，提供监控数据图表，比如某一段时间内的虚拟机在线数、平台的低负载率、以及平台的可用性等。

8.3.4.12 日志查询要求

1、具备海量的日志管理能力，提供精细化的日志查询，包括对设备的操作日志、账号权限的操作日志、用户行为的日志跟踪等。

2、支持管理员对系统安全预警、异常行为实时发现和严重事件实时响应。

8.3.4.13 配置管理要求

1、支持监控中心服务中的配置功能，对告警自定义阈值和告警订阅的配置。

2、支持对工单流程的各个环节进行配置，以及人员的配置。

3、支持定制租户使用监控中心的内容和处理异常的流程。

8.3.5 统一运维服务

8.3.5.1 基础管控层要求

8.3.5.1.1 文件分发与传输要求

文件分发传输应满足以下要求:

1、支持多种传输模式

（1）BT 模式：对于 10KB 上的文件分发自动启用 BT 作为首选传输方式，提升文件的分发效率以及避免拥塞。

（2）直传模式：针对 10KB 下（含 10KB）的文件使用 TCP 直传模式。

（3）混合模式：在 BT 模式传输持续性失败时，会尝试使用直传模式传输 BT 文件分片；当 BT 传输恢复时，停止直传模式。

2、支持多种传输类型

（1）文件传输：将多种格式、可读目录下的单个文件分发到指定机器；支持自动同步目标文件权限与源文件一致；对于直传模式，文件传输结束后进行 MD5 校验，对于 BT 模式和混合模式，支持哈希值校验文件的完整性。

（2）目录传输：用户将指定目录分发到多台机器指定可写目录下，目录分发将保持源目录结构和权限不变。

（3）正则匹配传输：支持用户通过通配符指定多个文

件，并传输到指定机器的指定可写目录，传输完成后文件的格式和权限与源文件保持一致。

3、支持多种传输控制方式

（1）区域链控制：支持通过设定规则，使文件只能在两个区域间单向传输，以满足具有特殊专线链接的两个区域间的传输需求。

（2）跨区域穿透：管控平台支持权限用户适当修改配置来完成定向穿透。

8.3.5.1.2 实时任务执行要求

实时任务执行应满足以下要求：

1、支持多种任务类型

（1）命令类型：Linux 支持 bash 命令、Windows 支持 cmd 命令、AIX 支持 ksh 命令，支持自定义可执行文件格式程序的启动，支持解释性语言程序的执行。

（2）脚本类型：Linux 支持 Shell 脚本、Windows 支持 bat 脚本（安装有 Cygwin 的额外支持 Shell 脚本）、AIX 支持 ksh 脚本，以及各种系统支持的解释性脚本程序。

2、支持多种任务控制方式

（1）指定用户： Linux 及其他类 Linux 系统支持按指定用户执行任务。

（2）继承用户环境： Linux 及其他类 Linux 系统支持指定用户后继承该用户设定的环境变量；Windows 可无此功

能。

（3）校验机器密码：用户选择校验机器密码，Windows Agent 按指定用户执行任务的功能。

（4）有害操作告警：管控系统能够自动设定高危操作的定义，并支持对高危操作进行预警。

（5）有害操作防护：管控系统支持自动识别高危操作，对高危操作预警和干预，高危操作的定义及干预措施提供选项供配置。

8.3.5.1.3 数据采集与分析要求

1、支持数据采集服务

（1）自定义数据采集：Agent 开放数据发送接口、cmdline 及 SDK，提供开发自定义数据采集程序或脚本。

（2）采集器插件化支持：Agent 支持采集器插件化，自动加载采集插件，并监控插件的存活状况。

（3）实时数据快照：基础管控层支持缓存安装有 Agent 的机器 1 分钟内的快照数据，并提供接口供用户访问。

（4）动态负载均衡：基础管控层支持按分钟级别动态调整数据转发通道。

2、支持集群管理

（1）自动服务发现：基础管控层同一个集群内的模块均支持自动发现，可以扩容、缩容任何节点，系统均能实时感知，并调整通讯策略，保证服务的高可用。

（2）集群负载均衡：基础管控层同一个集群内，支持按照 Agent 链接数进行负载均衡。

（3）多区域负载均衡：基础管控层支持对同一集群进行不同区域的划分，并按照各区域内的负载均衡规则处理。

3、支持元数据管理，如数据源和结果表的基本信息、血缘分析等。

4、支持数据清洗、实时计算、离线计算、日志检索等功能。

5、支持任务监控、数据监控、组件监控等功能。

8.3.5.1.4 主机管控要求

1、远程管控

支持跨云的管控，提供服务器 Proxy 模式管理远端服务器。

2、多操作系统兼容

支持 Windows、CentOS、RedHat、Debian、SUSE、Ubuntu、AIX、中标国产 Linux 操作系统。

3、批量管理

支持对多个主机的 AD、Oracle、VMware、网络、存储等对象进行批量管理，包括基本设置、配置获取、安装 agent 等。

8.3.5.1.5 自动化巡检要求

1、数据库巡检

支持对 Oracle、MSSQL、MySQL 数据库主流版本的自动化巡检。

2、中间件巡检

支持对 Tomcat、WebLogic、WebSphere 中间件自动化巡检功能。

3、安全保护

支持主流 Windows、Linux 系统自动化补丁修复功能，漏洞扫描功能，安全加固及安全基线比对功能。

4、巡检设置

支持按每日、每月或每年等时间条件进行周期性的巡检，同时支持巡检完成后发送邮件通知。

8.3.5.2 运维支撑层要求

8.3.5.2.1 灵活配置要求

灵活配置具体要求如下:

1、业务层面的主机资源管理

（1）支持外部资源的导入和云主机的实时同步;

（2）支持跨云管理主机;

（3）对于不同类型业务的主机资源，支持自定义属性的扩展功能。

2、业务管理

支持面向不同角色提供业务的权限级别管理和业务的增删改查等操作。

3、自定义属性管理

（1）支持基于业务、集群、模块和主机上新增自定义属性,。

（2）支持在 CMDB 中自定义主机属性时关联主机自定义采集策略。

4、进程端口与配置文件管理

支持将业务的进程、端口、配置文件注册到 CMDB，并关联到业务拓扑中，为上层的应用比如监控、进程管理等提供数据和配置服务。

5、对象管理

（1）支持需求自定义管理的对象类型，新增的对象类型可以关联到具体的业务拓扑。

（2）支持对应的增删改查 API 供周边系统使用。

6、资源分组

支持静态数据与动态数据两种配置数据，资源分组功能结合动静态数据对资源进行任意组合，供周边系统使用。

7、数据审计

支持数据审计，将动态数据与 CMDB 中的已存在静态数据进行周期性对比，当数据不一致时，进行告警并给出统一对比结果。

8、操作审计

支持 CMDB 上的操作都有对应的记录可供追溯，所有操

作审计记录都需录入到事件中心。

9、自动采集

支持与第三方自动采集器对接，实现数据采集。

8.3.5.2.2 运维作业要求

运维作业具体要求如下:

1、支持 Web 化脚本管理

（1）多协作者可以通过平台进行脚本共享使用。

（2）支持 Shell、BAT、Python、Perl、PowerShell、SQL 等脚本。

（3）支持自主开发脚本运维基本单元，以及将 API 接口开发成基本单元。

（4）多个脚本或文件传输流程可以串接组合成作业任务。

（5）支持服务器脚本远程执行。

2、支持批量高效执行

针对运维场景中的多服务器操作，提供并发执行任务的能力。

3、支持作业编排

将文件传输、脚本执行等步骤编排为作业流程，实现复杂场景下或跨系统的自动化作业执行。

4、支持任务定时

能够以秒为最小时间粒度制定定时任务计划，且每个定

时任务执行过程都会被记录日志，一切操作都可追溯。

5、支持维护工具开发

提供前端开发模版，以快速的实现各类运维工具的开发。

6、支持作业审计

按日期、操作人员、操作设备等条件提供详细的作业审计记录。

8.3.5.2.3 运维数据服务要求

1、支持数据接入、清洗、计算、存储、查询和分析的全流程自助化大数据服务。

2、支持通过统一数据接入、可视化计算任务配置、可视化建模、统一查询等功能快速地构建可视化、智能化的运维支撑工具。

3、支持快速构建基于大数据的可视化、智能化运维支撑工具。

8.3.5.2.4 智能数据分析要求

支持拖拽式建模、交互式测试调优、自动化模型评估、模型训练运行管理、场景模型（公共的通用的模型）等功能。实现各种基础的数据挖掘、机器学习算法节点化，将模型构建的过程标准化，让业务运维人员可以通过简单的拖拽配置完成数据分析工作。

8.3.5.3 统一集成层要求

8.3.5.3.1 支持多语言的开发框架

1、支持多语言的开发框架，平台支持 Python、php 等技术语言开发运维自动化工具。

2、支持开发框架集成统一登录鉴权模块、功能开关模块、WEB 安全防护模块、功能组件模块等通用模块。

8.3.5.3.2 免运维托管

1、支持从 SaaS 的创建、部署以及维护管理均免运维托管服务。

2、支持 SaaS 在平台采用分布式部署方式，一键自动部署。

3、支持 SaaS 部署使用 Docker 进行隔离，提高 SaaS 安全性。

4、提供查看日志记录和日志监控告警服务。

5、支持自定义配置告警参数、告警接收人等信息，实时监控日志数据。

8.3.5.3.3 企业服务总线&API GateWay

1、支持运维支撑层的各个支撑模块提供 API，统一以组件的形式对接企业服务总线，实现各支撑模块 API 的统一和集中化管理，在上层的应用可以通过企业服务总线调用 API。

2、支持在企业服务总线&API GateWay 上对组件的权限校验、频率控制、访问统计、路由分发以及自助接入等功能。

8.3.5.3.4 快速开发

提供丰富的 PC 和移动端的前端开发模版，运维开发人员可以利用丰富的前端开发模版，快速的实现各类运维工具的开发。

8.3.5.4 运维服务层要求

8.3.5.4.1 基础运维

支持运维工作中的日志查看、数值调整、数据提取、性能展示、配置变更等基础运维的自动化。

8.3.5.4.2 CI/CD

支持代码集成、构建、检查、测试 、布署、缺陷管理以及版本管理，实现全链路的自动化和可视化。

8.3.5.4.3 监控告警

支持主机性能、日志、自定义属性、应用性能、公共组件以及调用链等指标的监控告警,并对指标进行告警设置。

8.3.5.4.4 故障自愈

支持自定义和选择通用的收敛规则和自愈方案，对特定条件的异常告警进行收敛和防御，对特定条件的故障告警执行关联的自愈方案，在无人工干预的情况下实现故障治愈。同时提供告警处理查询、告警历史查询和告警数据统计等功能。

8.3.5.4.5 任务编排

支持原子的自助开发接入，实现各平台间的无缝连接，解决运维场景操作全流程的调度自动化。

8.3.5.4.6 弹性伸缩

根据容量、负载评估以及在线预测等智能决策模型，实现无人值守弹性伸缩。

8.3.5.4.7 安全审计

支持运维日常操作的高危扫描、行为监控、审计对帐，实现运维操作记录和操作结果的可追溯性。

8.3.5.4.8 移动运维

支持将部分简易固化的临时操作以及信息通知在移动端呈现，通过即时通讯工具的上下行实现部分交互的执行。

8.3.5.4.9 流程管理

支持 ITSM 工单流程管理以及可编排的流程引擎、多方式告警、企业微信审批、数据导出等功能，同时要求集成统一身份认证、单点登陆等功能和对接政务服务网、协同办公业务流程。

8.3.6 统一租户服务

8.3.6.1 租户权限管理要求

支持基于政府部门组织架构维度提供租户管理，实现与用户角色和权限体系的对接。

8.3.6.2 租户隔离和审计要求

1、支持每个租户对应单独的云账号，只有拥有云账号，才有权限访问云资源，实现租户资源的隔离。

2、支持每个用户都对应着子云账号，每个用户的操作

都会对应于云基础设施中的子云账号。区别每个用户的不同操作，便于对用户操作的审计。

8.3.6.3 租户配额要求

1、支持对租户进行云资源的配额管理。通过配额管理，实现有计划的、按量进行租户管理。

2、支持每个租户使用全部的云基础设施，没有量的限制。通过租户的配额管理，系统管理员可以给各个部门进行配额限制，对租户进行配额管理。

8.3.7 统一灾备服务

1、支持多租户通过WEB界面制定备份策略，管理子系统将备份资源池统一管理，按租户隔离，多租户的账号与云平台账号对接，实现统一认证。

2、支持用户和租户登录灾备管理平台实时监控备份系统运行情况，包括设备状态、客户端状态、备份/恢复作业状态等。

3、支持在报表的建立上，进行自定义，提供多维度多产品多服务的报表展现和统计计费功能。

4、支持灾备管理员对相关资源信息进行审批管理，包括资源的新增、修改、删除、查看等，并提供流程审批功能。

5、支持隔离备份资源，实现各业务单位的灾备系统资源隔离，每个租户仅能够访问与管理属于自己的虚拟灾备中心，对每个租户资源进行单独计费。

8.3.8 统一安全服务

统一安全服务具体要求如下:

1、支撑用户管理与用户隔离功能，确保用户间数据隔离与私密性。

2、支持通过软件定义网络 SDN 技术创建私有网络，私有网络间在二层 100%隔离，私有网络数量没有规模限制，增强二层网络的安全性及规模化应用，非使用 VLAN 技术控制广播。

3、支持 VPN，提供软件防火墙等、SSH 等安全机制，帮助用户防护非授权访问与攻击。

4、虚拟网络支持 ARP 多路径决策功能，防止大量 ARP 广播造成的泛洪问题。

5、虚拟网络设备需提供自定义安全组策略。

6、支持资源回收站功能，支持误删除资源找回，提供操作安全保证。

7、支持针对租户的虚拟化安全产品，虚拟防火墙、虚拟 WEB 防护（WAF）、虚拟 IPS 等。

8、对有安全管理需求的租户，必须提供独立的安全策略管理界面，方便租户进行按需的安全策略部署。

9、能够将安全资源与业务深度融合，实现东西向的流量防护，主要安全设备需支持 TRILL、VxLAN、OpenFlow 等标准化协议，具备国际标准的 SDN 功能，兼容第三方标准的

SDN 控制系统。

10、实现对安全事件的综合收集和分析，收集，如：防火墙、入侵检测等设备的事件信息和日志，并进行综合事件关联分析，发掘其中可能存在的安全隐患和安全事件。

11、提供的审计策略设置界面，使审计管理员可以选择三级安全应用支撑平台不同范畴中主客体访问的审计级别，并与访问策略、等级检查策略相配合，生成具体的审计策略，并将该策略发放给对应的安全部件。

8.3.9 统一适配平台

8.3.9.1 统一 API 接入管理要求

8.3.9.1.1 统一运营管理 API 要求

统一运营管理 API 要求如下:

1、统一服务目录

（1）要求云运营管理系统提供统一的服务目录。

（2）支持两类服务目录模式：云平台服务注册模式、运营管理系统自定义服务模式。

2、统一服务 Console

（1）支持 Console home 集成各子服务平台的服务 Console。

（2）支持各子服务平台将各自的平台服务 Console 注册至统一服务 Console。统一服务 Console 将定义统一的 Console 注册接口。

3、统一服务模板

（1）支持云服务的自定义功能，用户可以通过云运营管理系统自定义的服务申请云资源。

（2）支持各个子服务平台将服务资源申请参数按统一的模板格式注册到运营管理系统中，以便管理员根据服务模板定义并发布服务产品。

（3）各个子服务平台需提供产品资源申请 API 接口。服务模板中除了描述云服务资源申请参数，还可包括云服务的租户配置参数等。

4、统一租户配额配置

（1）运营管理服务系统应提供统一的租户配额管理的配置界面并通过 API 下发给各个子服务平台，各个子服务平台通过各自的租户配额管理模板控制各个租户的最大资源使用量。

（2）运营管理服务系统应从统一服务模板中获取各个云服务租户配额参数。

（3）各个子服务平台需提供租户配额配置 API 接口。

（4）运营管理服务系统支持两类配额管理模式：租户配额管理和 VDC 配额管理。

5、统一标签管理

（1）运营管理服务系统应提供统一的标签管理定义功能，各个子服务平台应使用运营管理服务系统的标签 API 给

本平台的资源打标签。

（2）支持统一标签管理，将定义统一的标签定义规范和 API 接口。

6、统一订单管理

（1）提供统一的订单服务接口，各个子服务平台在申请、变更、删除云资源时，调用订单相关的 API 生成订单，并根据最终的发放结果更新订单状态。

（2）云运营管理系统的统一订单管理模块收到来自各个子服务平台的订单提交接口,支持启动 VDC 配额管理控制。

（3）支持定义统一的订单提交 API 接口和订单完成 API 接口。

7、统一审批

提供统一的服务审批流程管理接口，各个子服务平台必须在申请、变更、删除云资源时，向云运营管理系统发起订单提交 API 接口，云运营管理系统根据预置的产品审批流程进行审批。

8、统一计量

支持统一的话单格式，各个云平台需要根据话单格式规范要求定期产生话单，并放到指定的服务器上，供云运营管理系统周期性采集。该接口将定义统一的计量规范格式。

9、统一操作日志

支持集中的操作日志服务，各个子服务平台需要调用统

一的操作日志 API 接口，集中记录操作日志。

8.3.9.1.2 统一运维管理 API 要求

统一运维管理 API 具体要求如下:

1、统一资源对象模型

提供可扩展的对象模型，并提供注册接口，各个子服务平台运维系统根据云运维管理系统定义规范。

2、统一告警管理

（1）支持集中的告警采集和呈现功能，提供统一的告警 API，各个子服务平台运维系统需要根据 API 格式规范要求上报告警。上报告警支持通用的协议,例如 SNMP 或 Restful 等。

（2）云运维管理系统采集到各个子服务平台的告警后，必须按租户、VDC、业务标签等多个维度展现给用户。

3、统一监控管理

支持周期性地向各个子服务平台的运维管理系统采集资源信息，各个子服务平台运维管理系统支持云运维管理系统定义的性能查询接口。

4、统一报表

采集到的资源、性能、告警相关数据，必须提供不同维度的报表给用户。

5、统一拓扑

支持根据资源信息以及资源的关系，提供不同维度的拓

扑，包括物理拓扑、逻辑拓扑等。

6、统一容量管理

基于采集的资源和性能数据，支持不同维度的容量统计信息，以便查看系统总体的使用情况和未来的使用趋势。

8.3.9.2 服务路由要求

支持调用的云账号，来决定后续应该路由至具体的子服务平台。

8.3.9.3 调用日志要求

API 调用操作，必须支持记录调用的日志情况，包括接口名称、提交报文、返回报文、异常情况、调用时长等。

8.3.9.4 安全审计要求

支持审计人员对适配平台上的各种接口调用、管理配置操作进行统一的审计。

8.3.9.5 服务限流要求

支持对单个云账号一段时间内的调用次数进行限制，根据预先的配置进行限流控制。

8.3.10 开放平台

8.3.10.1 统一身份认证要求

支持统一身份认证，第三方系统可使用统一身份认证进行登录集成。

8.3.10.2 统一权限管理要求

支持统一授权管理，包括菜单权限和数据权限，第三方

系统可注册到云管平台，定义系统菜单和数据范围，并能够对用户和角色进行菜单和数据的授权。

8.3.10.3 业务监控要求

支持业务方程序使用云管平台的监控能力，能够定义监控指标、指标告警配置、指标数据上报，云管平台负责数据处理、存储以及展示。

8.3.10.4 资源管理资源

支持对外开放资源管理 API，包括虚拟机、云存储、私有网络、负载均衡、浮动 IP、裸金属、数据库等 IasS、PaaS 资源。

支持对外开放管理能力 API，包括计镜像管理、机型管理、计算节点管理，虚拟化层管理等 API。

8.3.10.5 服务接入要求

1、支持 PaaS、SaaS 接入能力，统一由云服务门户展示 PaaS、SaaS 服务功能，根据服务特性、可配置计费和审批流程，用户在云管平台可以进行服务自助申请、配置、销毁操作。

2、支持接收服务实例的监控指标，进行统一的存储、预警和展示。

3、支持对服务实例进行计费。

8.4 接口要求

为了保证云平台的开放性，持续保证全省统一政务云技

术竞争力的目标，以及地市政务云平台拉通共享、资源融合，要求各地市政务云提供以 OpenStack 等开放的云平台为核心的接口能力，同时满足如下接口要求。

8.4.1 IaaS 对接

云管平台支持 IaaS 接入服务，主要有 API 对接和工单两种形式。

8.4.1.1 API 对接

使用场景如下:

1、租户资源管理，从云管调用 IaaS 接口进行资源创建，包括计算资源（虚拟机、弹性伸缩等）、存储资源（块存储、对象存储、文件存储等）、网络资源（私有网络、浮动 IP、虚拟网卡、安全组、防火墙、负载均衡等）。

2、基础资源管理，包括用户、租户、计算节点资源、机型、镜像等。为了达到对接要求，需要 IaaS 厂家按照云管要求开放接口，要求符合 OpenStack 标准，支持 K 版本至 P 版本。

（1）开放接口分为基础接口和高级接口:

包含基础数据的获取，虚拟机、云存储、网络资源的基本操作。资源使用者需从省云管界面进行资源申请，通过审批后，省云管调用地市云接口进行实际的创建操作。

（2）具体接口内容如下:

◎基础接口:机型 API、镜像 API、用户资源 API、租户

资源 API、计算资源 API、云存储资源 API、基础网络资源 API、安全组 API、虚拟网卡 API、浮动 IP API、防火墙 API、负载均衡 API、L3 路由器 API、对象存储 API。

◎基础增强型接口：计算资源管理 API、存储资源管理 API、网络资源管理 API。

◎高级南向接口：包含更多的资源操作及高级功能，接口内容有 QOS API、TAAS API、VPN API、文件存储 API、弹性伸缩 API、编排功能、裸机 API。

8.4.1.2 工单对接

云管平台提供工单系统，资源使用者可发起资源申请、变更。具体流程要求如下:

1、资源使用者登录云管工单系统，从服务目录选择需要的资源类型。

2、填写申请表，提交申请。

3、工单审批流程完成后，工单流转到地市云运维人员。

4、地市云运维人员进行资源发放操作，资源发放完后回填资源信息到工单系统。

8.4.2 服务对接

云管平台应支持 PaaS、SaaS 接入服务,第三方合作平台可以遵循云管平台要求，对服务进行服务开通、申请、管理、计费、定义审批流程等操作。

8.4.2.1 对接形式

PaaS 平台、SaaS 平台应集成到云管平台，分为租户侧和运维侧。

1、租户侧

资源用户登录云管平台，进行 PaaS 实例的申请、详情查看、管理、销毁操作，云管平台调用 PaaS 提供的 API 完成操作。

2、运维侧

PaaS 运维平台与云管平台通过单点登陆进行集成。运维用户登录云管平台，通过跳转链接可以直接到 PaaS 的运维平台；或者登录 PaaS 运维平台先跳转到云管平台进行身份认证。

8.4.2.2 租户侧对接

为了满足资源管理的需要，PaaS 需提供包括以下资源 API：资源创建、资源详情查看、资源管理操作、资源销毁。

8.4.2.3 运维侧对接

第三方合作平台开发者应用服务的登录模块要接入云管平台，主要要完成以下:

1、首次访问第三方合作平台开发者应用服务且用户尚未登录时，要展示云管平台的登录页面。

2、用户从云管平台登录后，再次访问第三方合作平台开发者应用服务时免登录。直接跳转到第三方合作平台开发者应用服务的主页

3、因云管平台的登录是基于同个 domain 下的 cookie 信息共享，在部署时须保证第三方合作平台开发者应用和云管平台在同一 domain 下。因此，用户从云管平台页面或者第三方合作平台开发者应用服务页面点击退出登录时，要清理整个 domain 下的 cookie。

8.4.2.4 服务监控对接

云管平台支持对服务器、网络设备进行监控数据采集和存储，第三方合作平台开发者可基于 API 接口定时上报监控数据，PaaS 服务上报每个 PaaS 实例的性能数据，由云管平台统一加工清洗数据处理，用户在云平台可以直接查看到 PaaS 实例的监控数据图表,实时展示业务稳定性监控数据。

8.4.3 监控对接

地市云的虚拟机需要安装 agent，收集虚拟机、业务系统的性能指标，供省云平台统一展示。

资源监控服务是针对云管平台计算资源和服务应用进行监控的一站式监控和告警。运维人员可以通过监控平台对物理设备、平台服务及平台运营状况进行统一管理和集中监控。除此之外，根据资源监控服务提供自定义配置的告警策略，及时获取异常信息，确保平台和资源的稳定运行。云监控平台主要有 8 大功能模块组成，它们分别是：总览、可视化、监控中心、性能服务监控、业务监控、系统运维、监控报表和配置管理。

8.4.4 资源上报

省级云管平台需要展示各地市 IaaS 的资源统计信息，对全省的云使用情况有一个总体的概览。云管平台提供标准接口，供地市上报统计信息，上报内容包括 CPU 统计信息、内存统计信息、存储统计信息、资源统计信息。