ICS 01.040.35
CCS L 70

DB11

北　京　市　地　方　标　准

DB11/T 2169—2023

政务云平台建设技术要求

Technical requirements for construction of government cloud platform

2023 - 12 - 25 发布　　2024 - 04 - 01 实施

北京市市场监督管理局　发布

目　　次

前言 II
1　范围 1
2　规范性引用文件 1
3　术语和定义 1
4　缩略语 2
5　云服务商要求 3
6　框架要求 3
7　建设要求 7
8　验收要求 17
9　监管要求 18
附录 A（资料性）　政务云平台服务技术指标 20
附录 B（资料性）　验收文档清单 28
附录 C（资料性）　政务云平台数据汇集（示例） 30

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。

本文件由北京市经济和信息化局提出并归口。

本文件由北京市经济和信息化局组织实施。

本文件起草单位：北京市大数据中心、紫光股份有限公司、阿里云计算有限公司、太极计算机股份有限公司、北京安信天行科技有限公司、中国电子技术标准化研究院。

本文件主要起草人：刘鹏、李佳、张琳、刘国伟、徐海琛、王岩、张颖、窦腾飞、崔建新、杨杰、宁振宇、籍志兵、朱向明、赵莹、万晓兰、金俊杰、丁明、唐道龙、尹斯、白强、丁冲、王惠琨、王璐、李巍、王忆柔、郑雅璐、陈青民、方莉莉、安亚鹏、王瑶瑶。

政务云平台建设技术要求

1 范围

本文件规定了云服务商要求、政务云平台框架要求、建设要求、验收要求和监管要求。

本文件适用于市级政务云管理单位、云服务商、云综合监管服务商及其他相关单位对政务云平台进行设计、建设、验收、监管等活动。区级政务云平台设计、建设等活动，可参照本文件。

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 22239 信息安全技术 网络安全等级保护基本要求

GB/T 31168 信息安全技术 云计算服务安全能力要求

GB/T 34077.3 基于云计算的电子政务公共平台管理规范 第3部分：运行保障管理

GB/T 34078.3 基于云计算的电子政务公共平台总体规范 第3部分：服务管理

GB/T 34078.4 基于云计算的电子政务公共平台总体规范 第4部分：服务实施

GB/T 34080.1 基于云计算的电子政务公共平台安全规范 第1部分：总体要求

GB/T 34080.2 基于云计算的电子政务公共平台安全规范 第2部分：信息资源安全

GB/T 34080.3 基于云计算的电子政务公共平台安全规范 第3部分：服务安全

GB/T 34080.4 基于云计算的电子政务公共平台安全规范 第4部分：应用安全

GB/T 37738 信息技术 云计算 云服务质量评价指标

GB/T 37972 信息安全技术 云计算服务运行监管框架

GB/T 39786 信息安全技术 信息系统密码应用基本要求

GB 50174 数据中心设计规范

GB 50462 数据中心基础设施施工及验收规范

3 术语和定义

下列术语和定义适用于本文件。

3.1

政务云平台 government cloud platform

为北京市属行政事业单位提供云基础设施、支撑软件和信息安全等综合服务的资源平台。

3.2

政务云管理单位 government cloud management unit

依据职责负责政务云的运行管理的单位。

3.3

政务云使用单位 government cloud user

政务云服务的使用方。

3.4

政务云服务商 government cloud service provider

政务云服务的供应方。

3.5

政务云综合监管服务商 government cloud comprehensive supervision service provider

受政务云管理单位委托，开展政务云运维监管、安全监管、应急管理和服务评价等工作的参与方。

3.6

云管理平台 cloud management platform

管理云计算服务的控制台。

4 缩略语

下列缩略语适用于本文件。

API：应用程序接口（Application Programming Interface）
CPU：中央处理器（Central Processing Unit）
DDoS：分布式拒绝服务（Distributed Denial of Service）
DNS：域名系统（Domain Name System）
FTP：文件传输协议（File Transfer Protocol）
HTTP：超文本传输协议（HyperText Transfer Protocol）
HTTPS：超文本传输安全协议（HyperText Transfer Protocol Secure）
IaaS：基础架构即服务（Infrastructure as a Service）
ID：身份标识号（Identity Document）
IMAP：因特网消息访问协议（Internet Message Access Protocol）
IOPS：每秒的读写次数（Input/Output Operations Per Second）
IP：互连网协议（Internet Protocol）
IPSec：互联网安全协议（Internet Protocol Security）
IPv6：互联网协议第6版（Internet Protocol version 6）
MAC地址：媒体存取控制地址（Media Access Control Address）
PaaS：平台即服务（Platform as a Service）
PM：物理机（Physical Machine）
POP3：邮件协议版本3（Post Office Protocol - Version 3）
PUE 数据中心消耗的所有能源与IT负载消耗的能源的比值（Power Usage Effectiveness）
SaaS：软件即服务（Software as a Service）
SDK：软件开发工具包（Software Development Kit）
SMTP：简单邮件传输协议（Simple Mail Transfer Protocol）
SSL：安全套接层（Secure Sockets Layer）
SYSLOG：系统日志（System log）
S/N：序列号（Serial Number）
TCP：传输控制协议（Transmission Control Protocol）
UPS：不间断电源（Uninterruptible Power Supply）
VFW：虚拟防火墙（Virtual FireWall）
VLB：虚拟负载均衡（Virtual Load Balance）

VM：虚拟机（Virtual Machine）
VPC：虚拟专有云（Virtual Private Cloud）
VPN：虚拟专用网络 (Virtual Private Network)
WAF：Web应用防护系统（Web Application Firewall）
WEB：全球广域网（World Wide Web）

5 云服务商要求

政务云服务商应满足如下要求：

a) 遵循 GB/T 31168 中云计算服务安全能力要求；
b) 具备政务云平台建设和运营经验；
c) 具备本地化服务能力，设置专职项目经理、运维人员，项目成员应具备项目管理、网络、安全、虚拟化、数据库、操作系统等专业知识和技能；
d) 具备 7×24 小时应急响应能力。

6 框架要求

6.1 总体框架

6.1.1 政务云总体框架如图1所示。

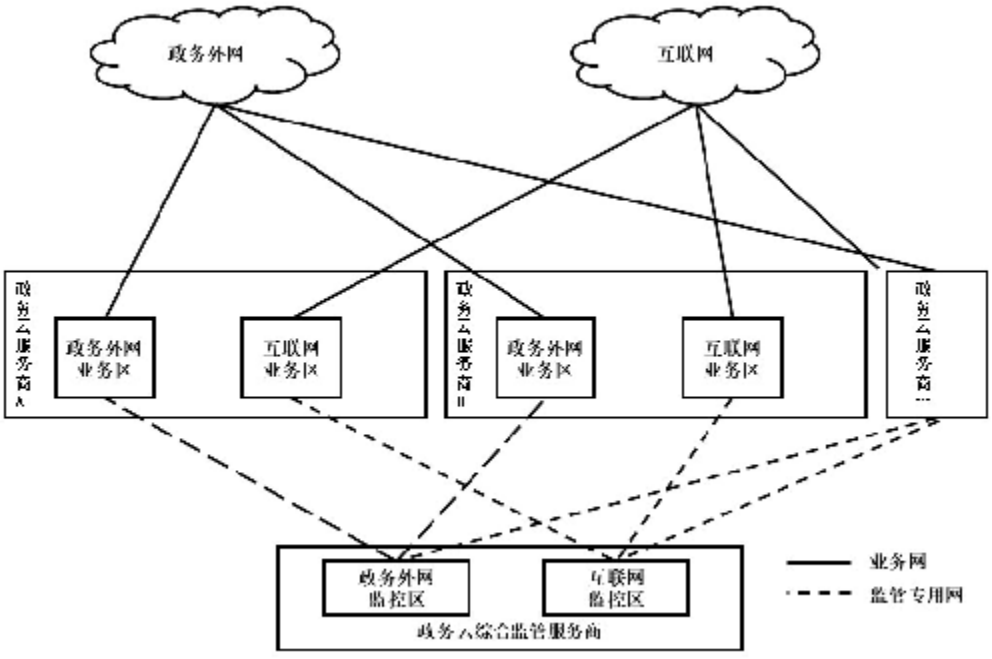


图1 总体框架

6.1.2 政务云服务商可跨机房提供统一的政务云服务，分别建设政务外网区和互联网区，并实现政务外网区和互联网区的隔离。各政务云服务商间各自独立建设并提供服务。
6.1.3 政务云综合监管服务商通过监管专用网络对政务云平台进行监管。

6.2 部署框架

6.2.1 各政务云服务商政务云平台逻辑部署框架如图2所示。

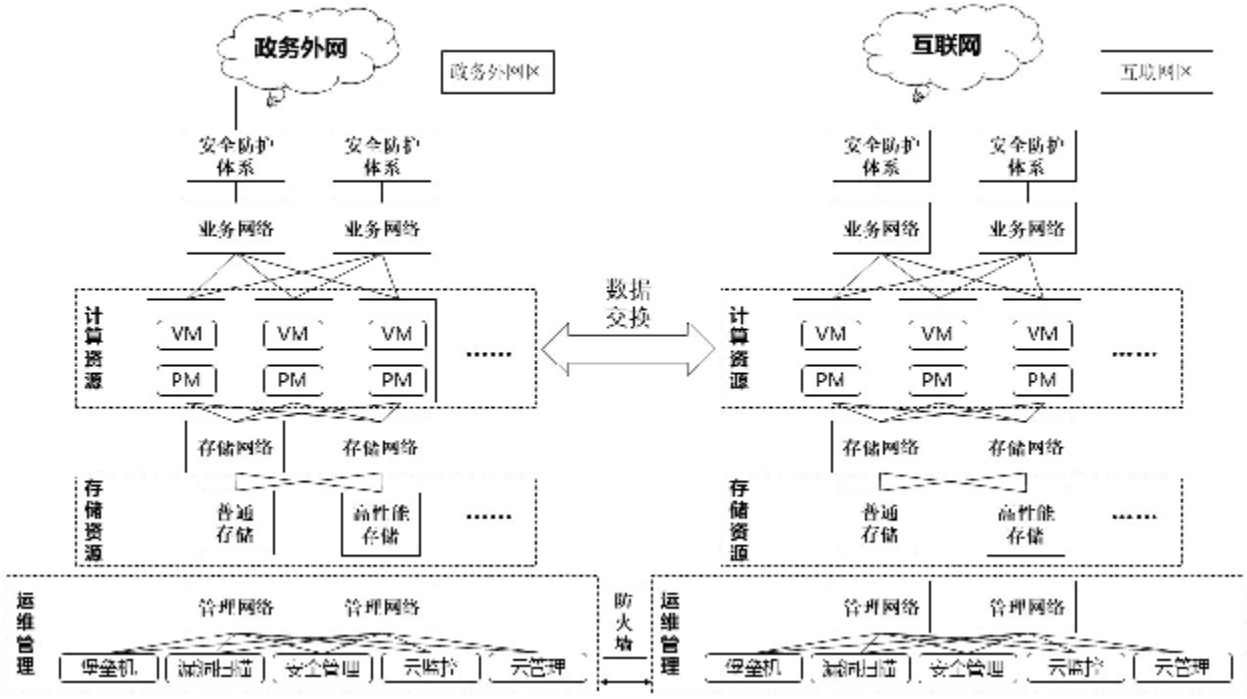
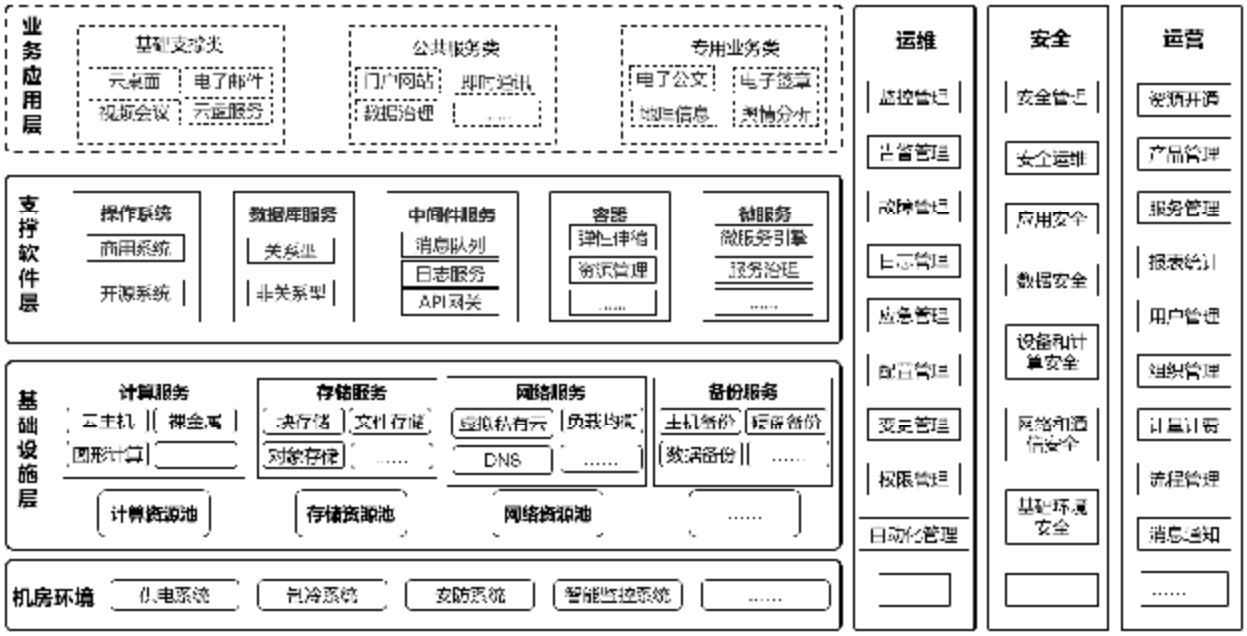


图2 部署框架

6.2.2 政务云平台部署应划分为政务外网区和互联网区，两区域间通过安全隔离，实现区域间的数据安全交换，通过安全防护体系进行统一管理。政务外网区和互联网区之间应隔离。内部业务区域为每个政务云使用单位划分不同的虚拟专有云（VPC）。

6.3 技术框架

6.3.1 政务云平台技术框架如图3所示，由机房环境、基础设施层、支撑软件层及业务应用层组成，在运维、安全和运营体系的保障下，为政务云使用单位提供统一服务支撑。



注：图中实线部分对应本文件相关规定，虚线部分仅为表明政务云平台技术框架的系统组成。

图3　政务云平台技术框架

6.3.2 应按如下内容设计具体架构：

a) 机房环境。为政务云提供安全、合规、完整的基础环境，应包含供电系统、制冷系统、安防系统、智能监控系统等；

b) 基础设施层。应采用分布式云基础架构，遵循分层、分模块解耦、统一接口调用的建设原则，通过虚拟化技术将计算、存储和网络等硬件设备进行资源整合，为政务业务应用提供基础资源服务；

c) 支撑软件层。为各类政务业务应用的开发、测试、部署、运行和运维提供统一的支撑环境，利用云原生、微服务及敏捷开发等技术，为应用上云提供可靠的工具支撑，保障业务稳定运行和敏捷迭代，包括但不限于容器、微服务、数据库服务、中间件服务以及操作系统服务等，并应支持统一管理；

d) 业务应用层。为满足政务云使用单位业务需求，政务云平台可提供共性的业务应用服务，业务应用层应包含基础支撑类、公共服务类和专用业务类等应用：

1) 基础支撑类应用包括但不限于云桌面、电子邮件、视频会议、云盘服务等；

2) 公共服务类应用包括但不限于门户网站、即时通讯、数据治理工具等；

3) 专用业务类应用包括但不限于电子公文、电子签章、地理信息、舆情分析系统等。

e) 运维。为保障政务云运维工作的标准化与规范性，政务云运维体系应是包含运维服务流程管理、基础设施运行监控、云服务监控的综合管理体系，实现监控管理、告警管理、故障管理、日志管理、应急管理、配置管理、变更管理、权限管理和自动化管理等；

f) 安全。为保障政务云全生命周期安全，应建立统一的安全管理、安全运维体系，保护云平台业务安全、数据安全和基础设施安全等；

g) 运营。运营平台是整个云数据中心的核心服务工具，实现对计算、存储、网络、安全等各类基础资源的生命周期管理，并将资源抽象为服务，实现服务的编排、交付和管理。同时为相关使用人员提供人机交互的工具，如门户控制台等。运营平台应实现对政务云所提供服务的统一管理，集中纳管各节点资源，实现可视化管理，主要包含资源开通、产品管理、服务管理、报表

统计等基础资源管理功能和用户管理、组织管理、计量计费、流程管理、消息通知等运营管理能力等。

6.4 服务能力框架

服务能力框架如图4所示，具体应包括：

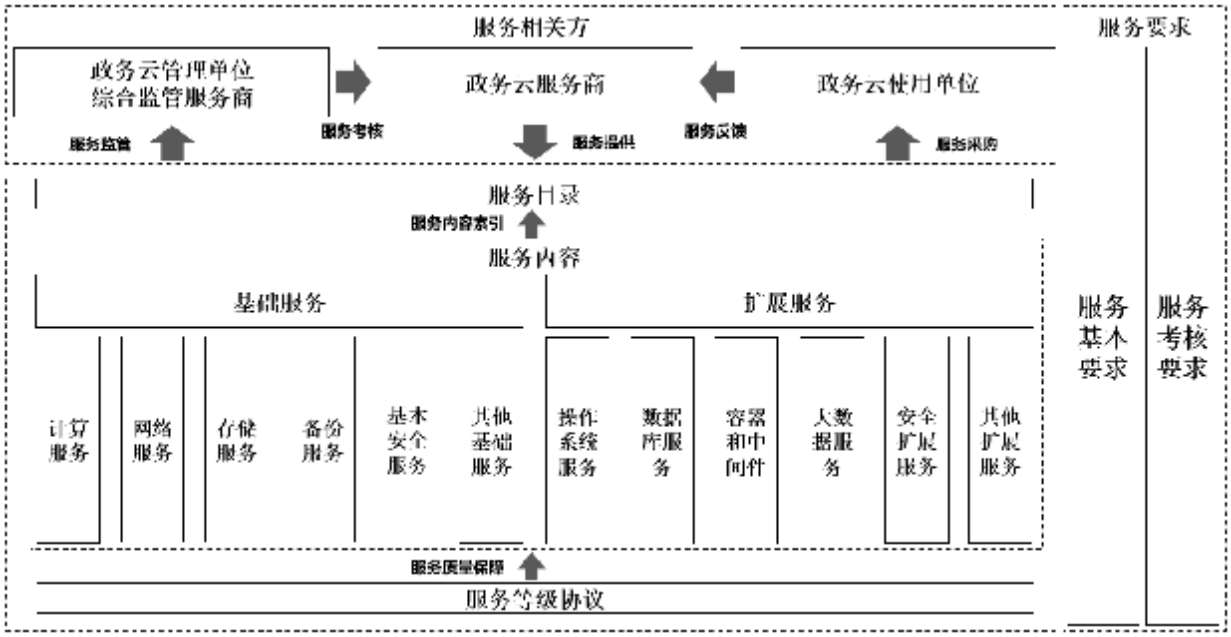


图4 政务云平台服务能力框架

a) 服务目录由政务云服务商提供，可满足使用单位信息系统运行需求的所有服务和服务产品的结构化信息，具体要求如下：
   1) 政务云平台可对外提供 IaaS、PaaS 类的服务项，分为基础服务、扩展服务两类；基础服务是云服务商必须具备的能力；扩展服务是云服务商可选择性具备的能力；
   2) 政务云服务商与使用单位通过服务合同约定的服务等级，包含服务定义、服务可用性等指标。
b) 服务要求包括服务基本要求、服务考核要求，具体要求如下：
   1) 服务基本要求，政务云所提供服务应满足的基本要求；
   2) 服务考核要求，对政务云所提供服务质量的考核性要求。

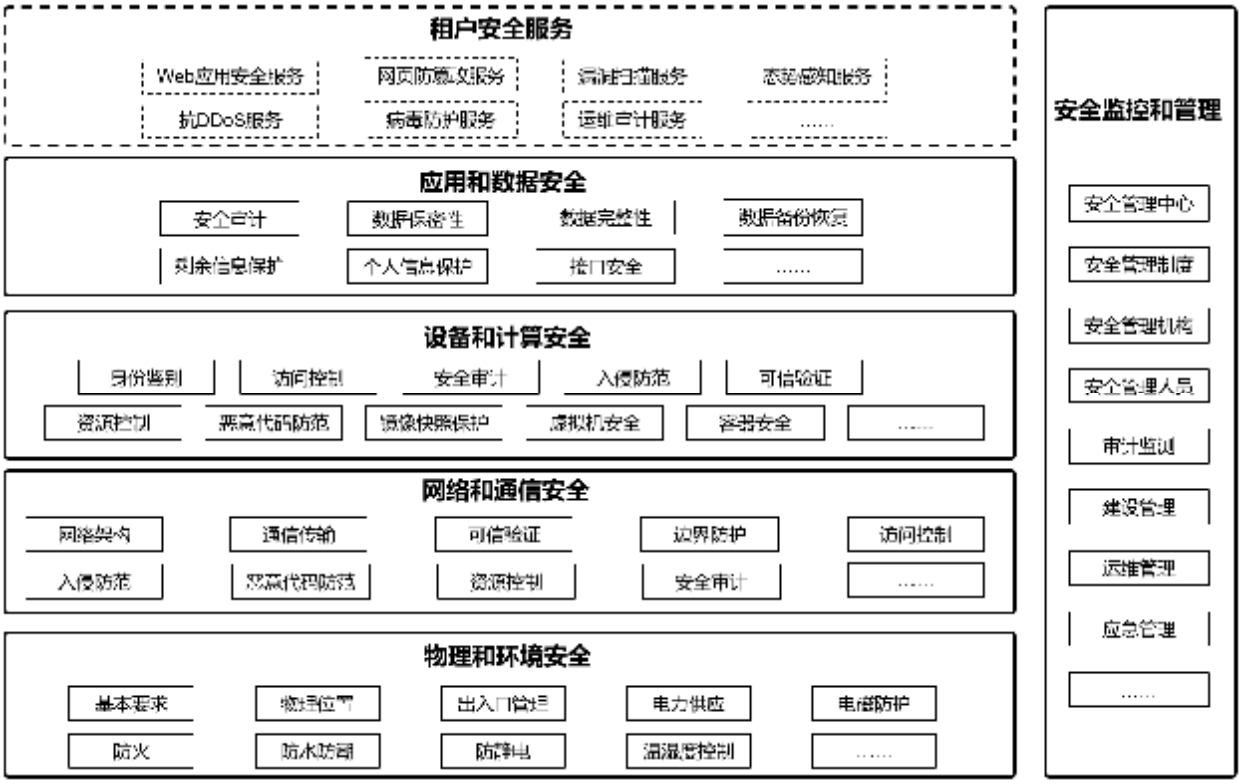
6.5 安全框架

政务云平台的安全框架如图5所示，具体应涵盖如下6个方面：

a) 物理和环境安全，涵盖物理环境的基本要求、位置要求、出入口管理、电力供应、电磁防护、防火、防潮防水、防静电、温湿度控制等方面内容；
b) 网络和通信安全，涵盖网络架构、通信传输、可信验证、边界防护、访问控制、资源控制、入侵防范、安全审计等方面内容；
c) 设备和计算安全，涵盖身份鉴别、访问控制、安全审计、入侵防范、可信验证、资源控制、恶意代码防范、镜像快照保护、虚拟机安全容器安全等方面内容；
d) 应用和数据安全，涵盖安全审计、数据保密性、数据备份恢复、剩余信息保护、数据完整性、接口安全等方面内容；

e) 安全监控和管理，涵盖安全管理中心、安全管理制度、安全管理机构、安全管理人员、审计监测、建设管理、运维管理、应急管理等方面内容；

f) 租户安全服务，租户安全服务可由政务云服务商提供，也可以由政务云服务商提供接口，供政务云使用单位购买第三方安全服务。



注：图中实线部分对应本文件相关规定，虚线部分仅为表明政务云平台安全框架的系统组成。

图5 政务云平台安全框架

7 建设要求

7.1 技术要求

7.1.1 整体要求

政务云服务商提供的云平台应满足如下要求：

a) 整体可用性不低于99.99%，数据可靠性不低于99.9999%；

b) 政务云全部设备，包括服务器、网络安全设备、服务器、存储 、安全设备等都应具备高可靠性及冗余性，即单个设备或单个节点出现故障时，其他设备/节点可立刻接管任务，保证云平台整体的业务连续性不低于99.99%。

7.1.2 机房要求

机房环境为政务云平台提供良好的运行物理环境，要求如下：

a) 应满足GB 50174 A级技术要求；

b) 地址应位于本市行政区域范围内；

c) 应具备为特殊用户需求划分独立物理区域的能力；
d) 实际运行 PUE 不高于 1.3；
e) 可用性应达到 99.9%；
f) 应配备建筑与结构系统、供电系统、制冷系统、网络与布线系统及消防系统；应设安防监控系统、场地环境与设备监控系统、火灾报警系统、自动控制系统并能够实时监控场地运行数据，视频监控数据保存不少于 3 个月；其他数据保存不少于 12 个月。

7.1.3 基础设施要求

7.1.3.1 功能要求

7.1.3.1.1 计算资源要求

计算资源提供的数据处理能力，要求如下：

a) 云主机应实现物理机的全部功能，如具有 CPU、存储、内存、网卡等资源，可以指定单独的 IP 地址、MAC 地址等；
b) 应支持存储裸设备映射（RDM），可以将存储设备上的 LUN 直接映射给虚拟机使用，并且支持 SCSI 指令使用透传模式或者非透传模式；
c) 云主机应支持多元计算服务，如 x86、ARM、GPU、NPU 等；
d) 应满足云主机之间、CPU 之间隔离保护要求；
e) 应支持资源的动态调整，根据业务的负载情况实现业务系统虚拟机的动态扩展和回收，支持手动和自动方式，自动方式可基于主机的 CPU、内存、磁盘 IO、网络流量等性能参数阈值进行动态调度；
f) 应支持在线进行虚拟化软件版本升级，不同版本之间可以相互兼容；
g) 应支持异构虚拟化能力，如 KVM、PowerVM 等多种虚拟化技术；
h) 云主机出现故障时，应支持自动重启或者迁移，保障业务连续性；
i) 应支持虚拟机热迁移，可在不同代 CPU 资源池中进行虚拟机热迁移。

7.1.3.1.2 存储资源要求

存储资源提供数据存储的能力，要求如下：

a) 应支持结构化数据、半结构化数据和非结构化数据等多种数据类型存储；
b) 应支持块存储、对象存储、文件存储等多种存储方法，满足数据备份、视频存储等不同应用场景使用要求；
c) 应支持存储资源扩展能力，例如：PB 级扩展；
d) 应支持磁盘容错技术，如磁盘故障后节点的自动平衡和重构、硬盘故障检测和处理、集群节点出现单盘故障时不影响业务运行等；
e) 应支持加密存储。

7.1.3.1.3 网络系统要求

网络系统提供数据传输能力，要求如下：

a) 应具备多运营商网络接入服务的能力；
b) 数据中心组网架构设计可采用大二层网络架构，应支持云主机无障碍动态迁移；
c) 应采用集群部署网络控制，以保障升级时业务不中断；
d) 应实现自动化动态网络资源调配和隔离，应支持与互联网、电子政务外网及行业部门专网的连接；

e) 应支持 IPv6 地址分配，满足业务系统 IPv6 要求；
f) 应具备边界防火墙和 VPC 防火墙隔离能力，分别针对不同的流量进行安全策略防护与配置；
g) 应具备高可用虚拟 IP 能力，在集群或主备场景下，云主机可绑定高可用虚拟 IP，达到高可用访问效果；
h) 应采用双活网络架构，降低单点故障带来的稳定风险；
i) 应为入云系统划分安全区域，合理制定访问规则。

7.1.3.2 性能要求

7.1.3.2.1 计算资源性能要求

计算资源性能要求包括但不限于如下：
a) 物理服务器 CPU 主频应不低于 2.4GHz；
b) 可用性不低于 99.99%。

7.1.3.2.2 存储资源性能要求

存储资源性能要求包括但不限于如下：
a) 存储系统的读写带宽应不低于 10Gb/s；
b) 应支持高可靠性，可靠性不低于 99.9999%；
c) 对于块存储服务，应支持普通性能、高性能两类，普通存储单盘技术指标：IOPS 大于等于 2000，高性能存储单盘技术指标：IOPS 大于等于 10000。

7.1.3.2.3 网络系统性能要求

网络系统性能要求包括但不限于如下：
a) 云内骨干线路带宽不低于 40Gb/s；
b) 服务器业务带宽不低于 10Gb/s；
c) 平均可用性不低于 99.99%。

7.1.4 支撑软件要求

7.1.4.1 总体要求

7.1.4.1.1 先进性要求

应采用先进的云计算技术及架构，以保证满足未来业务云化的技术发展要求。

7.1.4.1.2 可维护性、可扩展性要求

综合考虑应用软件、硬件结构，保证平台维护灵活、扩展便捷，同时应满足业务的各种上云需求。

7.1.4.1.3 安全、可靠性要求

政务云平台应具备高安全性，满足业务上云的动态接入安全要求，具备容错、检错、纠错能力，并具有快速恢复和重建能力，确保平台的连续可用性。

7.1.4.1.4 技术成熟度要求

政务云平台自身应基于成熟的、开放的技术架构体系，能够具备持续满足业务上云的各种应用服务的能力。

7.1.4.2 操作系统

操作系统是支撑政务业务应用的服务之一，应为云主机、裸金属等云服务提供操作系统镜像服务，要求如下：

a) 应提供各类主流的商用、开源操作系统，包括主流国产操作系统，并确保操作系统使用的合法性、安全性；
b) 应提供基于不同 CPU 架构的操作系统，以适应不同业务应用需要；
c) 应具备适配新型操作系统的能力。

7.1.4.3 数据库

7.1.4.3.1 一般要求

数据库为政务业务应用等提供数据存储能力，要求如下：

a) 应支持关系型数据库及非关系型数据库；
b) 关系型数据库应支持集中式数据库与分布式数据库两种架构；
c) 应支持主流的商业、开源操作系统，包括主流国产数据库；
d) 应支持数据库服务化管理，提供数据库全生命周期的管理能力；
e) 应支持对数据库监控、告警等。

7.1.4.3.2 关系型数据库

关系型数据库是指采用了关系模型来组织数据的数据库，其以行和列的形式存储数据。

a) 集中式的关系型数据库要求如下：
   1) 应具备基于集群及负载均衡等技术的能力；
   2) 应支持多种资源部署模式，如裸金属、云主机、容器等；
   3) 应具备数据库的备份能力与集群的容灾能力。
b) 分布式的关系型数据库要求如下：
   1) 事务型数据库应能抵御网络问题导致分布式数据库服务脑裂风险；应支持跨库死锁检测；应支持数据分片在线拆分；
   2) 分析型数据库应支持对地理信息（GIS）与时序数据进行存储和分析；应支持标准云原生存算分离架构。

7.1.4.3.3 非关系型数据库

非关系型数据库是基于高可用架构，满足高读写性能及快速数据访问需求的分布式内存数据库，要求如下：

a) 应支持内存和硬盘的持久化存储方式；
b) 应支持多种资源模式部署，如：云主机、裸金属、容器等；
c) 应支持虚拟网络，指定虚拟网络创建内存数据库实例；
d) 应支持在线平滑升降级，计算能力、内存容量和总 I/O 带宽同步线性扩容；
e) 应支持缓存服务的容灾。

7.1.4.4 中间件

7.1.4.4.1 概述

中间件为业务提供应用支撑能力，包括但不限于消息队列、日志服务及API网关。

7.1.4.4.2 消息队列

消息队列是构建分布式应用的基础设施，消息队列应实现松耦合架构设计，以提高系统可用性以及可扩展性，功能要求如下：

a) 应提供分布式消息队列服务；
b) 应支持发布订阅模型；
c) 在单个消息生产者情况下，应支持顺序消息，包括消息的顺序发送与顺序接收；
d) 应提供日志记录功能；
e) 应支持主流的消息队列服务，如：Kafka、RabbitMQ；
f) 应具备完善的多用户隔离机制，保障用户数据的私密性；
g) 应具备权限控制白名单机制，用户只能访问其角色配置过的 topic，无权限访问其他 topic；
h) 应具备跨 Region 消息队列之间数据同步能力；
i) 应能为每个消息服务提供单独命名空间，保证政务云使用单位间数据严格隔离；
j) 应提供优先级队列功能；
k) 应提供对消息加密功能；
l) 应支持消息的跨集群容灾能力；
m) 应支持节点主机配置双网卡，实现安全隔离；
n) 应支持配置数据同步功能，在不同消息队列集群之间持续提供数据同步服务。

7.1.4.4.3 日志服务

日志是发现问题、定位问题的重要信息，应提供统一的日志平台服务，具体要求如下：

a) 应提供统一收集 PaaS 平台组件的日志服务；
b) 应提供收集面向应用的日志服务，如应用定向写到文件中的日志；
c) 应提供对日志的可视化管理、组合过滤查询的能力；
d) 应支持用户自定义解析规则和解析规则组，并预制多种解析规则实现日志数据解析；
e) 日志数据冷热数据分离存储，支持分别配置冷数据和热数据保存时间，也可支持永久保存；支持自定义日志分片数和副本数；为了提高存储资源利用率，支持日志投递功能，按 JSON、CSV 等转存格式转储日志数据到共享存储。

7.1.4.4.4 API 网关

API网关提供API托管服务，覆盖设计、开发、测试、发布、售卖、运维监测、安全管控、下线等API各个生命周期阶段，具体要求如下：

a) 应支持创建、发布、上线、监控、下线等 API 的全生命周期管理能力；
b) 应支持可视化的 API 编排，以无代码可视化的方式编排 API 接口；
c) 应支持 HTTPS 接入访问；
d) 应支持配置接口缓存策略，对于匹配的接口请求，可直接由缓存数据响应，以减轻后端业务服务的访问压力；
e) 应支持按接口、按组织、按应用和按源 IP 的多种灵活限流策略，从不同维度对接口的访问进行秒、分钟、小时、天的多种时间单位的流量控制。

7.1.4.5 容器

7.1.4.5.1 资源管理

容器云服务提供以容器为核心的容器管理服务，为容器化的应用提供高效部署、资源调度、服务发现等一系列完整功能，具体要求如下：

a) 应具备资源管理能力；
b) 应具备多集群管理能力；
c) 应具备多租户管理能力；
d) 应具备运维系统、监控系统等基本功能；
e) 应具备自动清理闲置容器镜像能力，并可自定义最大保留时长；
f) 通过升级检查后，应支持自动化低版本容器管理平台向高版本升级，通过升级检查后，可进行全自动化。

7.1.4.5.2 弹性伸缩

容器云服务提供以容器为核心的动态伸缩功能，具体要求如下：

a) 应提供资源分配与调度功能，包括统计资源利用率，并能够按照策略动态分配资源；
b) 应提供容器动态迁移功能，包括伸缩迁移、故障迁移等功能；
c) 应支持容器通过手工和自动方式的弹性伸缩。

7.1.4.6 微服务

7.1.4.6.1 微服务引擎

微服务引擎是微服务注册中心和配置管理的全托管式平台,提供高可用且免运维的服务注册和配置管理集群，具体要求如下：

a) 应支持 SpringCloud、istio、Dubbo 等主流开源框架；
b) 应提供服务发现接口，用以对服务和资源进行发现；
c) 应支持微服务组件的启动、停止、升级、弹性伸缩、删除等管理，且支持可视化查看微服务组件运行状态、异常告警、健康检查；
d) 应支持微服务注册中心、配置中心和 API 网关一键创建，创建时可选择多实例保障服务可用性。可指定各组件所占用的资源配额，可自定义配置中心后端的数据库地址、API 网关后端的数据库和缓存。

7.1.4.6.2 微服务治理

微服务治理用于实现各个微服务的自动化注册与发现，具体要求如下：

a) 应支持多种负载均衡路由策略，如：随机，轮询，会话保持等；
b) 应支持服务降级策略，包括：屏蔽降级和容错降级，以保证核心服务的 SLA；
c) 应提供调用链监控，生成调用链数据，记录链路的各项性能指标，包括吞吐量、响应时间、错误记录等，支持调用链数据存储及查询；
d) 应支持根据服务名查看对应的实例，选择时间窗口后可查看到单位时间的请求量、成功率、平均响应时间、响应最慢的 10 个接口等。

7.1.5 运维能力要求

运行维护管理应符合GB/T 34077.3以及IT服务管理等，主要包括以下内容：

a) 监控管理：应提供监控场所和监控终端，应对机房、网络、主机、存储、软件等资源的运行状况进行监测、记录和趋势分析，对监控记录进行保存，保存周期至少半年；

b) 告警管理：应支持对业务系统相关的告警进行趋势分析、时序分析，可分层次查看告警详情，告警可与业务拓扑联动。应支持通过多种方式进行告警提醒，并支持告警转流程工单，在工单中查看告警对象的实时运行状态；
c) 故障管理：应支持分析故障的根本原因，找出解决方案，将故障进行汇总，并纳入问题库，预防故障的再次发生；
d) 配置管理：应支持对云资源进行统一的配置管理，包括集中调度、分级分域管理、按需弹性分配资源等，支持多级审批配置，支持审批人员变更；
e) 权限管理：应提供用户的权限管理功能，支持管理员角色的调整查询，支持管理员分权分域管理，支持政务云操作系统的单点登录功能，登录密码满足政务云使用单位业务的安全需求。

7.1.6 安全保障要求

7.1.6.1 总体安全技术要求

政务云平台总体安全技术要求如下：
a) 应保证安全技术服务能力不低于所承载的信息系统的最高级别，并通过 GB/T 22239 相应等级的测评；
b) 应符合 GB/T 34080.1，GB/T 34080.2，GB/T 34080.3，GB/T 34080.4 中的规定；
c) 应通过商用密码应用安全性评估，商用密码应用安全性评估参考 GB/T 39786 中相应等级规定；
d) 应保障其上的租户安全、容器安全、云主机安全、业务安全和数据安全；
e) 在服务期内，承载政务云平台的软硬件应在原厂维保期限内。

7.1.6.2 物理和环境安全

政务云平台的物理和环境安全具体要求如下：
a) 物理和环境安全要求应符合 GB 50174，GB 50462 和 GB/T 34080.1 的规定，并按照 GB/T 39786，GB/T 22239 中不低于等保三级的物理和环境安全要求执行；
b) 应确保政务云平台所有设备及承载的业务和数据均位于北京市内运行。

7.1.6.3 网络和通信安全

政务云平台的网络和通信安全具体要求如下：
a) 网络和通信安全要求应符合 GB/T 22239 中的不低于等保三级的关于安全通信网络和安全区域边界的规定，并按照 GB/T 39786 中不低于等保三级的网络和通信安全要求执行；
b) 应能够绘制与当前运行情况相符的虚拟化网络拓扑结构图，并应能对虚拟化网络资源、网络拓扑进行实时更新和集中监控和管理。

7.1.6.4 设备和计算安全

政务云平台的设备和计算安全具体要求如下：
a) 设备和计算安全要求应符合 GB/T 22239 中不低于等保三级的关于安全计算环境的规定，并按照 GB/T 39786 中不低于等保三级的网络和通信安全要求执行；
b) 应支持屏蔽虚拟资源故障，如：某个云主机崩溃后不影响云主机监视器及其他云主机；
c) 云主机仅能使用为其分配的计算资源；
d) 应确保云租户业务应用系统的虚拟机内存空间安全；
e) 应提供基本的容器安全防护措施，确保容器镜像来源可信、容器仓库连接安全、容器镜像和容器仓库的风险可管理、容器运行风险可监测。

7.1.6.5 应用和数据安全

政务云平台的应用和数据安全具体要求如下：

a) 应用和数据安全要求应符合 GB/T 22239 中不低于等保三级的关于安全审计、可信验证、数据完整性、数据机密性、数据备份恢复、剩余信息保护、个人信息保护的规定，并按照 GB/T 39786 中不低于等保三级的应用和数据安全要求执行；
b) 应保证不同云租户的应用系统及开发平台之间的隔离；
c) 保证不同云租户的审计数据隔离存放；
d) 应保证政务云资源和应用服务对外接口的安全性。

7.1.6.6 安全监控和管理

政务云平台的安全监控和管理具体要求如下：

a) 政务云平台资源审计监测应符合 GB/T 34080.2-2017 中第 7 章的规定；
b) 政务云平台安全管理中心建设、安全管理制度建设、安全管理机构设置、安全管理人员管理以及政务云平台的建设管理、运维管理和应急管理等安全管理要求应符合国家标准 GB/T 22239 不低于等保三级的安全要求规定，并按照 GB/T 39786 中不低于等保三级的关于管理制度、人员管理、建设运行和应急处置相关要求执行。

7.1.6.7 租户安全服务

以云服务目录的方式为云租户提供云安全服务，具体要求如下：

a) 政务云平台应具备为云租户提供自有和第三方云安全服务的能力；
b) 宜支持为云租户提供云安全服务，如 Web 应用防护、网页防篡改、抗 DDOS 服务、漏洞扫描、运维审计、态势感知、病毒防护等安全服务；
c) 宜支持软件安全设备、硬件安全设备混合构建安全资源池，混合后的安全资源池作为一个整体资源池可分配给不同租户使用；
d) 宜具备安全服务弹性扩展能力，能够通过服务器数量的增加提高承载安全组件的规模和性能；
e) 宜支持云主机配置迁移策略，避免因物理主机故障导致资源不可用。

7.1.7 运营能力要求

7.1.7.1 总体要求

政务云服务商应使用云管理平台对所运营的政务云资源、政务云使用单位和服务进行统一管理。云管理平台应满足政务云平台的以下基本技术要求：

a) 应支持平台管理节点集群部署，并可平滑升级扩展；
b) 应支持同构资源池的多节点管理；
c) 应支持自服务门户，用于政务云使用单位自主管理所用云资源，提供资源监控、资源操作等基本能力；
d) 应支持运营门户，用于政务云服务商运营管理云资源，提供组织管理、权限管理、计量计费、统计分析及服务管理等基本能力；
e) 应支持与政务云监管平台对接。

7.1.7.2 接口规范要求

7.1.7.2.1 概述

政务云平台应提供标准的接口，包含但不限于管理平台、虚拟化平台、网络、安全、存储系统等接口，具备纳管相关物理设备及系统的能力，提供标准的南向接口和北向接口功能及标准文档规范。

7.1.7.2.2 南向接口

南向接口主要是基础设施层的接入，对云资源和服务进行统一纳管，包含但不限于：

a) 硬件接入应提供物理设备的接口，包括服务器设备、网络设备、存储设备等。
b) 软件接入要求：
    1) 应遵循 Restful 风格，可以查询政务云平台服务状态信息、云平台物理资源使用情况等；
    2) 应提供政务云使用单位相关的增、删、改、查等接口；
    3) 应提供云主机的相关接口，包括虚拟机云主机详细信息、列表、快照、硬盘规格、镜像等；
    4) 应提供存储资源相关的接口，包括云硬盘、硬盘快照、访问鉴权等；
    5) 应提供虚拟网络资源相关的接口，包括网络、子网、网卡、虚拟路由、安全组、公网 IP、VFW、VPN、VLB 等。

7.1.7.2.3 北向接口

北向接口主要是云管理平台的开放接口，以实现云管理平台能够被第三方应用开发、部署和安全监管，包含但不限于：

a) 应提供丰富的 REST API 接口供第三方在云操作系统上进行业务应用开发部署，提供的接口涵盖基础设施、支撑软件和业务应用各个层面，实现一个开放的云服务平台；
b) 应提供多种安全监管接口，以提供相关安全监管数据。安全监管接口类型包括网络流量接口、网络协议接口、云主机接口和 API 等。

7.2 服务内容要求

7.2.1 基本要求

政务云平台的服务内容技术设计等应符合GB/T 34078.3和GB/T 34078.4中的规定。

7.2.2 服务目录

政务云平台的服务应由政务云服务商以目录形式统一对外公布，一般宜每年更新一次。

7.2.3 服务等级

政务云服务商以服务等级协议的方式，向使用单位明确提供对应服务的服务可用性等级指标，并按照相关服务等级协议执行，以保障对应服务稳定运行。

7.2.4 服务内容

7.2.4.1 概述

服务内容包括基础服务和扩展服务，详细技术指标见附录A。

7.2.4.2 基础服务

基础服务应包含计算服务、存储服务、网络服务、备份服务、基础安全服务：

a) 计算服务，应提供云主机、物理主机租用、图形图像计算等服务；
b) 存储服务，应提供普通性能存储、高性能存储服务；

c) 网络服务，应提供互联网链路、主机负载均衡、远程接入、SSL VPN、IPSec VPN、SSL 证书、WAF 防护等服务；
d) 备份服务，应提供本地备份、本地/异地视频云存储、视频数据备份链路等服务；
e) 基础安全服务，应提供云主机深度监控、安全攻击威胁监测等基础服务。

7.2.4.3 扩展服务

7.2.4.3.1 扩展服务包含操作系统、数据库、容器和中间件、安全扩展等服务，具体如下：

a) 操作系统服务，宜提供商用操作系统、开源操作系统等服务；
b) 数据库服务，宜提供关系型数据库（集中式、分布式）、非关系型数据库（Redis、MongoDB 等），以及数据仓库、数据库工具（数据传输、数据管理、数据库备份等）等服务；
c) 容器和中间件服务，宜提供容器（Kubernetes 容器、Serverless 容器、服务网格、边缘容器、容器镜像等）、微服务（微服务引擎、分布式应用、云服务总线和 API 网关、应用配置管理等）、消息队列（Kafka、RabbitMQ 等）、应用高可用、链路追踪、业务实时监控等服务；
d) 扩展安全服务，宜提供租户安全（DDoS 防护、漏洞扫描、入侵检测、安全评估、渗透测试等）等服务。

7.2.4.3.2 云服务商宜提供应用迁云、性能测试、性能调优、深度巡检、重要时期保障、全链路压测、专项咨询等服务，以扩展服务等形式提供运营支持，包括：

a) 应用系统上云，提供应用兼容性评估、上云基础架构设计、上云实施技术支持、迁移风险策略控制等服务；
b) 云上应用调优，提供应用架构诊断、分库分表设计、微服务治理、云原生改造等服务；
c) 全链路压测，提供压测方案设计、实施支持、优化服务等服务；
d) 重要时期保障，提供深度健康检查、预防式维护、应急保障计划、高级别现场维护与故障处理等服务。

7.2.5 服务考核

云服务质量评价的基础性指标应符合GB/T 37738确定的安全性、可用性、可靠性、响应度、满意度、可保障性要求。

7.3 扩展能力要求

7.3.1 概述

扩展能力是指满足当前建设要求的前提下，具备按照政务云管理单位、政务云使用单位的要求进行扩展开发的能力，一般包括云平台扩展、系统对接扩展等。

7.3.2 云平台扩展能力要求

根据政务云管理单位、政务云使用单位的要求，对云管理平台进行相应扩展开发，要求如下：

a) 应支持对计算资源、网络资源、存储资源、安全资源自动化调度及管理；
b) 应对云资源使用情况进行计量管理；
c) 应支持云资源账单记录、费用预估和分析等管理；
d) 应支持资源总览、使用分析、整体优化等活动；
e) 应提供服务目录、工单管理、报表管理、权限管理、运行数据管理和汇集、策略管理调度与分配、信息发布、知识库和云主机网络接口带宽检测等功能；
f) 应支持云服务统一门户，支持统一的接入入口与现有的业务系统进行集成；

g) 应支持大屏展示模块，包括政务云运行状态、资源情况、运维事件等展示功能；
h) 应支持大屏扩展模块，包括多维度指标的按需展示和用户自定义编排；
i) 应支持运维管理模块，包括运维门户、监控、报表等的按需开发，并支持自定义展示；
j) 应支持运营模块，包括申请审批流程、组织管理、多级审批等按需开发。

7.3.3 系统对接扩展能力要求

根据云管理单位、使用单位的要求，对云管理平台与其他系统进行对接，不断拓展政务服务能力，要求如下：

a) 应支持标准的 RESTful API 接口，通过接口将各服务商提供的各项功能与其他平台进行互联互通；
b) 应具备第三方设备的异构兼容开发能力，包括硬件、安全设备等；
c) 应具备第三方产品的快速部署对接能力，包括 SaaS 类应用的镜像上传、安装部署和运维监控等能力；
d) 应具备第三方管理平台的对接能力，包括安全管理、运维管理、监管平台等；
e) 应具备生态场景的对接能力，包括平台设施、中间件、数据库、业务逻辑、UI 等；
f) 应提供对接操作的规范性流程，包括：
   1) 明确业务过程，明确政务云服务与第三方服务之间业务关系；
   2) 明确接入方式，如协议方式、SDK 方式等；
   3) 明确接口信息，应根据业务场景，明确需要接口调用的具体数据信息；
   4) 制定规范性文档，根据以上列项 1-3，与第三方平台沟通确认后，制定接入规范性文档，政务云服务根据接入规范进行对接；
   5) 接入联调，按规范性文档，接入第三服务，并对接入的服务进行双方联调；
   6) 接入完成，根据请求信息完成配置后，完成接入。

8 验收要求

8.1 总体要求

政务云平台验收包括初验、试运营和终验三个阶段，要求如下：

a) 初验是政务云平台初步完成建设并具备基础服务能力后开展的阶段性验收，初验通过后可与政务云监管平台进行对接，并进入试运营阶段；
b) 试运营是按照政务云管理单位的要求开展云平台试运行阶段，政务云管理单位可检验相关运营和技术能力情况，并提出整改要求，以确保政务云平台符合建设要求，当政务云平台通过政务云管理单位要求的国家相关安全合规性检查后可申请终验；
c) 终验是政务云平台完成试运营阶段后，由政务云管理单位按照验收关键指标和整改要求，检验相关验收材料的完整性、符合性，通过终验后，政务云平台可正式提供政务云服务。

8.2 验收组织

由政务云服务商组建验收组织，组织成员至少包含政务云管理单位、安全领域专家顾问、政务云使用单位及其他相关人员。

8.3 验收内容

8.3.1 初验

当政务云服务商完成政务云平台的初步建设并具备基础服务能力后可以向政务云管理单位申请进行初验。验收内容如下：

a) 审查政务云平台基础功能和性能指标是否实现，包括基础服务目录及相关服务的功能和性能；
b) 审查业务支撑文档，包括用于指导政务云使用单位使用政务云的指导资料，以及用于内部运维的规范方案等，初验文档清单见附录 B.1；
c) 审查与政务云监管平台的对接计划、政务云平台扩展功能实现计划；
d) 其他事项，如机房环境的合规性等。

8.3.2 终验

8.3.2.1 当政务云服务商建设的政务云平台通过政务云管理单位要求的国家相关安全合规性检查后可申请终验。验收关键指标如下：

a) 审查政务云平台是否完成政务云管理单位要求的国家相关安全合规性检查；
b) 审查政务云平台对第七章建设要求的满足情况，包括技术要求、服务内容要求和扩展能力要求等；
c) 审查政务云服务商试运营阶段的整改情况。

8.3.2.2 验收文档清单见附录 B.2。

9 监管要求

9.1 总体要求

政务云服务商应遵循政务云管理单位统一的运维监管要求和安全监管要求，做好政务云平台日常运维工作、变更管理、应急管理、重要时期保障、政务云平台可用性监测以及安全事件的监控和处置。同时，应按照监管数据汇集要求向政务云管理单位提供运行数据，并提供监管要求落实的管理和技术证明材料，证明材料应符合GB/T 37972要求。

9.2 数据汇集要求

9.2.1 基本要求

政务云服务商应通过自动化和手工机制向政务云管理单位提供云平台运行数据和监管数据，政务云管理单位对汇集数据进行统一管理。汇集数据应结合政务云管理单位的管理目标和内容进行详细定义，汇集数据相关示例见附录C。

9.2.2 监管数据汇集框架

政务云平台运行数据和相关监管数据的获取方式包括：手工机制和自动机制。自动机制环境下，从数据获取的接口形式来说，可分为网络流量接口（NFLOWI）、网络协议接口（NPROTI）、云主机接口（VMI）和应用程序编程接口（API）4种类型，手工机制通过数据填报的方式来实现。政务云管理单位汇集监管数据形成监管数据中心，并对汇集数据进行应用开发，作为监管工作的支撑平台，从而对政务云服务商进行持续监管。监管数据汇集框架如图6所示。

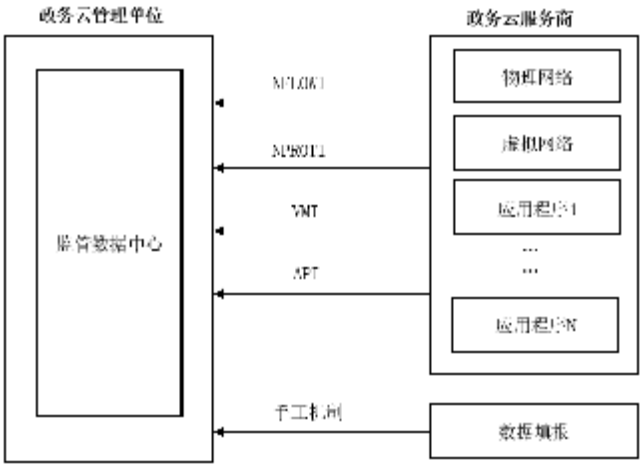


图6　监管数据汇集框架

9.2.3　资产数据

应包括但不限于物理环境资产数据、物理设备资产数据、云主机资产、IP资产、用户资产（入云系统）等，实现对各类资产状态和数量的实时监控数据。

9.2.4　机房环控数据

应包括但不限于温湿度传感器、门禁、发电机、电池监控模块、UPS等设备运行及状态数据。

9.2.5　网络协议数据

应包括但不限于TCP协议、HTTP/HTTPS协议、DNS协议、SMTP协议、POP3协议、 IMAP协议和FTP协议等数据。

9.2.6　日志数据

应包括但不限于安全设备日志和主机日志等数据。

9.2.7　云平台数据

应包括但不限于云平台规格数据、云平台网络接入IP地址数据等。

9.2.8　应用数据

应包括但不限于业务系统数据、云主机规格数据、互联网链路带宽服务数据等。

9.2.9　监控数据

应包括但不限于运行监控数据、应用系统网络出口使用数据、VPN远程接入登录数据等。

附 录 A
（资料性）
政务云平台服务技术指标

A.1 云主机技术指标

表A.1给出了云主机技术指标。

表A.1 云主机技术指标

序号	指标项	指标描述	基线值
1	性能限制	云主机 CPU 性能指标	CPU 主频≥2.4GHz CPU 核数≥1 核
2		虚机系统磁盘空间	≥40GB
3		云主机内存，按内存不复用方式	≥1GB
4	性能范围	CPU 核数可选范围	1~64 核
5		内存可选范围	1~128GB
6		虚机数据磁盘空间范围	20GB~32TB
7	扩展性	用户可以灵活调整云主机 CPU、内存、硬盘规格	-
8	云主机隔离	对不同用户的虚拟主机提供安全组或 VLAN 级别的隔离，确保不同用户之间数据互不可见	-
9		云主机之间可以做到隔离保护，其中每一个云主机发生故障都不会影响同一个物理机上的其他云主机运行，每个云主机上的用户权限只限于本云主机之内，以保障政务云平台的安全性	-
10	HA 功能	云管理节点需支持双机热备等高可用方式	-
11		云主机具有高可用（宕机迁移）功能，硬件设备出现故障时，在其上运行的云主机能够在其他正常的物理节点上重新启动，保障业务的连续性	-

A.2 物理服务器租用服务技术指标

表A.2给出了物理服务器租用服务技术指标。

表A.2 物理服务器租用服务技术指标

序号	指标项	指标描述	基线值
1	性能要求	CPU 性能指标	CPU 核数≥16 核 CPU 主频≥2.4GHz
2		内存性能	≥16GB
3		内存数量	≥4 个
4		磁盘空间	≥480GB
5		万兆网口	≥2 个
6		HBA 板卡	≥2 个
7	管理权限	用户对物理服务器有完全的控制权，具有管理员权限	-
8		保障管理权限不外漏，物理主机的物理接入需提请运维单 按照管理规定进行申请流程	-
9		存放物理服务器的机柜应支持物理钥匙	-
10	可操作性	支持通过云管理平台，实现申请部署与使用	-
11		支持通过云管理平台，监控主机运行状态	-

A.3 图形图像计算服务技术指标

表A.3给出了图形图像计算服务技术指标。

表A.3 图形图像计算服务技术指标

序号	指标项	指标描述	基线值
1	基础要求	基于计算平台提供图形计算服务	-
2	性能要求	GPU 规格	GPU 显存≥1GB
3		单精度浮点计算能力	≥0.15TFLOPS
4	可操作性	支持通过云管理平台，实现申请部署与使用	-

A.4 普通性能存储服务技术指标

表A.4给出了普通性能存储服务技术指标。

表A.4 普通性能存储服务技术指标

序号	指标项	指标描述	基线值
1	可靠性	提供普通存储服务，要求稳定可靠，可通过分布式或副本数据冗余保护等方式，提高数据可靠性	99.9999%
2	性能要求	单盘技术指标满足IOPS要求	IOPS≥2000
3	使用要求	最小分配容量	20GB

表 A.4 普通性能存储服务技术指标（续）

序号	指标项	指标描述	基线值
4	使用要求	用户可以将申请到的磁盘空间同时分配给一台或者多台云主机/物理机使用	-
5	架构要求	系统整体架构无单点故障	-
6	可操作性	支持通过云管理平台，实现申请部署与使用	-
7	存储读写带宽	存储系统的读写带宽	≥10Gb/s

A.5 高性能存储服务技术指标

表A.5给出了高性能存储服务技术指标。

表A.5 高性能存储服务技术指标

序号	指标项	指标描述	基线值
1	可靠性要求	可靠性程度	≥99.9999%
2	性能要求	单盘技术指标	IOPS≥10000
3	使用要求	最小分配容量	20GB
4		用户可以将申请到的磁盘空间同时分配给一台或者多台云主机/物理机使用	-
5	架构要求	系统整体架构无单点故障	-
6	可操作性	支持通过云管理平台，实现申请部署与使用	-
7	存储读写带宽	存储系统的读写带宽	≥10Gb/s

A.6 总体网络服务技术指标

表A.6给出了总体网络服务技术指标。

表A.6 总体网络服务技术指标

序号	指标项	指标描述	基线值
1	可靠性要求	平均可用性	≥99.99%
2	骨干线路带宽	云内骨干线路带宽	≥40Gb/s
3	服务器业务带宽	服务器业务带宽	≥10Gb/s

A.7 互联网链路服务技术指标

表A.7给出了互联网链路服务技术指标。

表A.7 互联网链路服务技术指标

序号	指标项	指标描述	基线值
1	带宽租用服务	提供互联网带宽租用服务，带宽提供方应为一级运营商	-
2		云服务商应与一级运营商签订的链路租用合同	-
3	可靠性要求	须提供两条或两条以上不同运营商接入服务，保证服务稳定可靠	-

表 A.7 互联网链路服务技术指标（续）

序号	指标项	指标描述	基线值
4	互联网IP地址租用服务	可提供IPV4/IPV6互联网IP地址租用服务	-
5		满足业务系统IPV6改造要求	-
6	网站域名备案服务	配合使用单位完成网站域名备案	-
7	可操作性	支持通过云管理平台，实现申请部署与使用	-

A.8 远程接入服务技术指标

表A.8给出了远程接入服务技术指标。

表A.8 远程接入服务技术指标

序号	指标项	指标描述	基线值
1	功能要求	提供堡垒机远程接入服务	-
2		堡垒机冗余部署	-
3		租户运维与平台运维独立部署堡垒机	-
4	运维审计	字符操作审计、图形操作审计、文件操作审计	-
5		运维审计操作日志、远程接入及运维审计设备日志保留时间	≥6个月
6	访问控制	支持基于IP/IP段、用户/用户组、资产/资产组、协议、危险级别、运维账号登录时间等策略进行访问控制，对于不合法的行为予以阻断	-
7		支持双因子认证登录功能	-
8		应支持粒度为端口级别的访问控制策略	-
9		应支持加密传输的访问方式	-

A.9 SSL VPN 服务技术指标

表A.9给出了SSL VPN服务技术指标。

表A.9 SSL VPN 服务技术指标

序号	指标项	指标描述	基线值
1	接入方式	实现Web接入，TCP接入，IP接入等多种方式，支持通过SSL-VPN远程接入专有网络，记录完整的用户访问日志	-
2	身份管理	支持基于用户身份的管理，实现不同身份的用户拥有不同的命令执行权限	-
3		支持用户视图分级，对于不同级别的用户赋予不同的管理配置权限	-
4	密码要求	通过商用密码产品认证	-

A.10 IPSec VPN 服务技术指标

表A.10给出了IPSec VPN服务技术指标。

表A.10 IPSec VPN 服务技术指标

序号	指标项	指标描述	基线值
1	配置方式	通过手工配置或自动配置的方式实现IPSecVPN隧道的建立，支持IPsecVPN建立专有网络到政务云使用单位本地数据中心的VPN连接，支持对IKE策略、IPSec策略配置及对VPN服务、IPSec站点连接的申请并提供状态监控，记录完整的用户访问日志	-
2	基本功能	实现 IPsec 抗重放检测功能、反向路由注入功能，支持IPv6 协议。包括创建、修改、删除连接	-
3	密码要求	通过商用密码产品认证。支持IKEv1和IKEv2协议，同时支持API方式配置	-

A.11 SSL 证书服务技术指标

表A.11给出了SSL证书服务技术指标。

表A.11 SSL 证书服务技术指标

序号	指标项	指标描述	基线值
1	SSL证书服务	提供域名SSL证书服务，可支持服务器、负载均衡等设备部署配置，实现数据信息在客户端和服务器之间的加密传输，可以防止数据信息的泄露，保证信息传递的安全性	-

A.12 WAF 防护技术指标

表A.12给出了WAF防护技术指标。

表A.12 WAF 防护技术指标

序号	指标项	指标描述	基线值
1	检测算法	可精确识别OWASP Top 10 WEB通用攻击，有效应对盗链、跨站请求伪造等WEB特殊攻击	-
2	部署方式	可以通过透明串接或反向代理、路由模式等方式接入网络中，即可对应用层HTTP流量进行安全防护	-
3	黑名单	通过预定义策略及自定义规则，进行规则匹配，阻断异常流量	-
4	可操作性	支持通过云管理平台，实现申请部署与使用	-

A.13 操作系统技术指标

表A.13给出了操作系统技术指标。

表A.13 操作系统技术指标

序号	指标项	指标描述	基线值
1	操作系统	Debian、Red Flag Asianux、凝思、湖南麒麟、银河麒麟、中标软件、中兴新支点、统信UOS、CentOS、EulerOS、Fedora、Linux Mint、openSUSE、Scientific Linux、Ubuntu、Windows等	-

A.14 数据库技术指标

表A.14给出了数据库技术指标。

表A.14 数据库技术指标

序号	指标项	指标描述	基线值
1	数据库	Kingbase（人大金仓数据库）、KDB、DM(达梦数据库)、GaussDB、PolarDB、Mysql、PgSQL、Redis、MemeCache、MongoDB、MariaDB、HBase、SQLite等	-

A.15 备份服务技术指标

表A.15给出了备份服务技术指标。

表A.15 备份服务技术指标

序号	指标项	指标描述	基线值
1	备份管理	备份方式	全量备份、差异备份和增量备份
2		备份时间段	非业务窗口时间
3		具备高可用性和冗余性	-
4		支持Windows系列操作系统、Linux主流系统操作系统、国产操作系统、主流数据库软件、主流大数据软件、主流中间件软件、结构化数据以及非结构化数据等备份对象	-
5		支持建立统一的备份管理系统，用来管理本地备份和异地备份	-
6		云服务商应提供对备份过程状态、备份结果的运维监控保障服务，确保备份任务执行成功以及备份的数据完整性	-
7		备份传输过程应支持加密传输能力	-
8		备份文件应支持加密存储功能	-

A.16 基础安全保障服务技术指标

表A.16给出了云主机深度监控服务技术指标。

表A.16 云主机深度监控服务技术指标

序号	指标项	指标描述	基线值
1	时间监控	监控时间连续性	7×24h
2	监控内容	应支持内存、CPU、磁盘、网络、防病毒等	-

表 A.16 云主机深度监控服务技术指标（续）

序号	指标项	指标描述	基线值
3	集中告警	支持多维度告警/事件展现	-
4	性能监控	CPU告警阈值	80%
5		内存告警阈值	80%
6		磁盘告警阈值	80%
7		网络接口带宽阈值	80%
8	安全事件服务	提供主机安全事件的验证、分析，并提供事件报告	-
9	应急响应	应急服务	7×24h
10		平均响应时间	≤15m
11		平均故障恢复时间	≤30m
12	值守保障	值守时间连续性	7×24h
13		值守内容不仅限于机房巡检、云平台和硬件监控，同时提供问题排查协助、协助处理应用故障等服务，并提供相应报告	-

A.17 主机负载均衡服务技术指标

表A.17给出了主机负载均衡服务技术指标。

表A.17 主机负载均衡服务技术指标

序号	指标项	指标描述	基线值
1	服务能力	通过云管理平台实现针对每租户按需自动分配负载均衡服务的能力。提供4层TCP/UDP和7层HTTP/HTTPS协议类型的服务	4 层新建连接数/秒≥30 万 4 层并发连接数≥1000 万 4 层吞吐量≥20Gb/s 7 层 HTTP QPS≥6 万 7层HTTPS QPS≥2万
2	均衡策略	支持加权轮询(Weighted Round Robin)、加权最小连接数调度(Weighted Least-Connection Scheduling)等流量分发策略。支持4层一致性hash、轮询(RR)，加权轮询(WRR)和最小连接数(WLC)等调度算法	-
3	健康检查	可以按照指定规则对配置的虚拟主机进行健康检查，自动隔离异常状态虚拟主机，确保可用性	-
4	会话（Session）保持	可对虚拟主机提供TCP/HTTP协议的负载均衡服务，调度算法4层支持TCP源地址会话保持，7层支持HTTP Cookie会话保持。在会话生命周期内，将同一会话请求转发到同一台后端虚拟主机	-
5	高可用性	采用全冗余或集群架构，无单点故障	-
6		平均可用性	≥99.99%
7	转发规则	提供多种转发规则，满足不同业务场景的要求	-

A.18 本地/异地视频云存储技术指标

表A.18给出了本地/异地视频云存储技术指标。

表A.18 本地/异地视频云存储技术指标

序号	指标项	指标描述	基线值
1	可靠性	数据可靠性要求	≥99.9999%
2		可靠性演练	半年一次
3	架构要求	容量扩展能力	EB级别

A.19 视频数据备份链路技术指标

表A.19给出了视频数据备份链路技术指标。

表A.19 视频数据备份链路技术指标

序号	指标项	指标描述	基线值
1	可靠性	提供音视频等数据进行备份的链路带宽服务，要求链路质量稳定可靠，保证备份工作在备份窗口内完成。至少每年进行一次备份数据恢复演练	-

附 录 B
（资料性）
验收文档清单

表B.1给出了初验文档清单。

表B.1 初验文档清单

文档目录	文档分类	文档名称
1	设计方案	政务云平台建设方案
2		政务云平台设计方案
3	证明报告	国家A级电子信息系统机房设计和建设证明（社会机房需要提供）
4		开工报告
5		第三方机构提供的政务云平台建设要求符合性测评报告
6	施工计划	政务云平台施工组织计划
7		政务云平台交付组织计划
8	设计图纸	机柜及环控设计布置图
9		设备清单竣工拓扑
10	功能/安全测试	政务云平台功能测试记录
11		政务云平台安全测试记录
12	云平台服务能力证明	政务云平台基础服务目录能力说明
13		政务云平台运维服务能力说明（运维保障方案、运维服务团队）
14	流程指导规范	政务云服务商服务水平规范
15		政务云运维工作方案及流程
16		政务云业务系统迁移技术指导方案
17		政务云平台安全管理方案（入云安全）
18		政务云平台应急预案
19		政务云内业务系统应急预案及应急演练指导书
20	规划文件	项目例会会议纪要
21		试运营工作计划
22		与政务云监管平台的对接计划
23		政务云平台扩展服务实现计划

表B.2 终验文档清单

表B.2给出了终验文档清单。

文档目录	文档分类	文档名称
1	证明报告	试运营阶段运行及整改报告
2		项目总结报告
3		政务云平台通过等保三级测评报告
4		政务云平台通过国密测评报告
5		与政务云监管平台的对接报告
6		政务云平台扩展服务目录能力说明

附 录 C
（资料性）
政务云平台数据汇集（示例）

C.1 数据汇集接口

政务云平台监管数据汇集接口如表C.1所示。

表C.1 政务云平台监管数据汇集接口

一级接口分类	二级接口分类	数据描述	数据汇集结果
网络流量接口NFLOWI	物理网络接口	政务云服务商应提供政务云平台物理网络中核心交换机和接入交换机的物理网络接口流量，用于监测、审计政务云平台安全事件、安全威胁等安全监管工作	网络协议数据
	虚拟网络接口	政务云服务商应提供政务云平台的虚拟交换和路由设备接口，以获取设备中使用的协议列表、源 IP 地址列表、目标 IP 地址列表、服务端口、数据流向等信息。所提供的虚拟交换和路由设备接口，应支持可以根据指定策略将指定流量牵引到政务云管理单位指定的监测设备，用于监测、审计等工作	网络协议数据
网络协议接口NPROTI	Syslog接口	政务云服务商应开启政务云平台物理网络中服务器、网络设备、安全设备等的 Syslog 接口，通过网络将syslog消息发送到政务云管理单位指定的监管设备上	日志数据
	SNMP接口	政务云服务商应开启政务云平台网络、安全设备的SNMP协议管理接口，使得政务云管理单位能够获取政务云所有网络及安全设备的运行信息	日志数据
	以太网接口	政务云服务商应为政务云管理单位的监管工作分配合适的以太网接口，保证在实施监管技术检测时能监测到监管对象，综合监管技术实施措施可通过以太网口接入政务云平台网络，开展云平台安全监管技术工作（例如：漏洞扫描），并获取技术检测/监测数据	-
云主机接口VMI	云主机接口	政务云服务商应提供虚拟云主机接口用于对虚拟资源性能状况进行抽样监测	-
应用程序编程接口API	应用程序编程接口	政务云服务商应根据政务云管理单位的监管要求，按需提供 API 接口，以便获取支撑综合监管工作开展的基础数据。（依据政务云管理单位的实际要求，选择自动机制或者手工机制）	资产数据 机房环控数据 云平台数据 应用数据 监控数据
手工机制	数据填报		

C.2 资产数据

汇总政务云服务商政务云平台物理资产数据如表C.2所示。

表C.2 资产数据

数据分类	数据内容描述	范围
物理环境/设备资产	云平台物理设备名称、设备S/N（序列）号、品牌名称、设备型号、硬件规格、IP地址、设备所在机房、所在机柜、设备功率、电源类型、设备所有单位、设备管理单位、运行状态、启用日期、撤出日期等	物理环境资产包括机房、机柜等。物理设备资产包括服务器、存储、网络交换、安全设备等
云主机资产/用户资产	入云系统名称、虚机资产、IP地址、使用单位系统管理人、管理员联系方式、系统入云时间、服务启用/撤离时间	云平台的入云系统和云主机资源使用情况

C.3 机房环控数据

机房环控数据如表C.3所示。

表C.3 机房环控数据

数据分类	数据内容描述
温湿度传感器	设备所在机房、所在位置、温度数据、湿度数据
发电机	设备编号、所在位置、故障状态、油位容量、运行状态
电池监控模块	设备编号、所在机房、所在位置、电流数据、总电压数据、后备时间
UPS	设备所在机房、所在位置、输入频率、环境温度数据、环境湿度数据、输出频率、电池总电压、电池总电流、电池温度、电池后备时间、电池剩余容量、电池总电流、UPS供电状态、UPS运行状态、电池运行状态、市电输入告警状态、电池告警状态
采集器	设备所在机房、所在位置、漏水状态、红外状态、继电器输出数据
列头柜	设备所在机房、所在机柜编号、A/B/C相电压、A/B/C相电流、A/B/C相负载率
电量仪	设备所在机房、所在位置、总有功电度量、总无功电度量

C.4 网络协议数据

采集TCP、HTTP/HTTPS、DNS、SMTP、POP3、IMAP、FTP等协议的数据，如表C.4所示。

表C.4 网络协议数据

数据分类	数据内容描述
TCP	时间戳（第一个包的时间，绝对时间）、入库时间、采集引擎名称、采集节点名称、采集节点类型、源 IP 地址及端口、目的 IP 地址及端口、连接状态、连接次数、会话总长
HTTP/HTTPS	时间戳（第一个包的时间，绝对时间）、入库时间、代理 IP 地址、采集节点名称、采集节点类型、源 IP 地址及端口、目的 IP 及端口、主机名、请求全路径、返回码、真实 IP 地址、COOKIE、请求方法、HTTP 类型、请求头、响应头、响应服务器名、请求内容、响应内容、入流量、出流量
DNS	时间戳（第一个包的时间，绝对时间）、入库时间、代理 IP、采集节点名称、采集节点类型、源 IP 地址及端口、目的 IP 地址及端口、查询域名、DNS 类型、查询类型、请求类型、返回码、请求资源类型、资源记录被缓存的秒数、域名级别、响应数据、响应数据长度、资源记录数、请求域名数量、顶级域名、额外资源记录数、授权资源记录数
SMTP/POP3/IMAP	时间戳（第一个包的时间，绝对时间）、入库时间、代理 IP 地址、采集节点名称、采集节点类型、源 IP 地址及端口、目的 IP 地址及端口、邮件类型、邮箱账户、加密状态
FTP	时间戳（第一个包的时间，绝对时间）、源 IP 地址及端口、目的 IP 地址及端口、传输模式、文件名称、文件 MD5 值

C.5 日志数据

采集政务云平台物理网络中的安全设备日志、云主机日志数据，如表C.5所示。

表C.5 日志数据

数据分类	数据内容描述
安全设备日志	日志产生日期、日志报警名称、安全设备发生源 IP 地址、安全设备代理 IP 地址、安全设备名称、设备 S/N 号、设备类型、源 IP 地址及端口、目的 IP 地址及端口、日志等级、报警类型、日志内容
主机日志	云主机日志（例如创建）产生日期、云主机 ID、主机名称、主机 IP 地址、操作系统类型、日志名称、日志类型、日志正文内容

C.6 云平台数据

政务云服务商提供政务云平台的整体管理数据，如表C.6所示。

表C.6 云平台数据

数据分类	数据内容描述
云平台规格数据	云服务商名称、设备所在机房、云平台产品供应商、云平台网络类型（政务外网/互联网）、CPU总量、CPU分配量、内存总量/分配量、普通存储总量/分配量、高性能存储总量/分配量、静态存储总量/分配量、互联网带宽总量/分配量
云平台网络接入IP地址数据	网络类型（政务外网/互联网）、云服务商名称、设备所在机房、网络运营商、IP地址/IP地址段、主链路带宽数、备份链路带宽数

C.7 应用数据

政务云服务商统计本单位负责的政务云平台入云信息系统的基本情况，如表C.7所示。

表C.7 应用数据

数据分类	数据内容描述
业务系统数据	政务云使用单位编号、单位地址及邮编、云服务商名称、所属节点、设备所在机房、信息系统编号、入云测试日期、系统联系人姓名、系统联系人手机号、系统联系人邮件地址、系统联系人座机、技术联系人姓名、技术联系人手机号、前置审批情况、系统功能描述、系统等保级别、运行时间要求、系统服务对象、系统服务范围、所属网络类型（政务外网/互联网）、系统互联网情况及涉及单位、上线日期、退出日期、退出原因、系统IP地址、系统开发商名称
云主机规格数据	信息系统编号、云主机名称、云主机ID、内部IP地址、云主机类型、云主机运行状态、云平台所属服务商、云主机设备所在机房、云主机所属网络类型（政务外网/互联网）、云主机创建/删除日期、CPU核数、内存分配量、平台存储分配量、高性能存储分配量、本地视频存储分配量、异地存储分配量、云主机深度监控服务情况
互联网链路带宽服务数据	信息系统编号、互联网IP地址、系统域名、互联网带宽数、互联网带宽接入起始时间、互联网带宽接入截止时间
主机负载均衡服务数据	信息系统编号、内网IP地址、外网IP地址、负载IP地址、开放端口、负载开通日期、负载关闭日期
VPN服务数据	信息系统编号、VPN类型、账号名称、可访问范围（IP地址或IP地址段）、VPN开通日期、VPN关闭日期
WAF防护服务数据	信息系统编号、WAF所防护IP地址及端口号、WEB防护类型（默认或自定义）、WAF防护开通时间、WAF防护关闭时间
远程接入服务数据	信息系统编号、远程接入账号名称、可访问范围（IP地址或IP地址段）、远程接入开通日期、远程接入关闭日期
云机房专线接入服务数据	信息系统编号、网络运营商、专线用途、专线接入起始时间、专线取消结束时间、线路本端（云平台端）地址、线路对端地址、配线柜编号、云机柜编号、接入设备名称及端口号

C.8 监控数据

政务云服务商向政务云管理单位提交本单位所负责的政务云平台的监控数据如表C.8所示。

表C.8 监控数据

数据分类	数据内容描述
云主机监控数据	云主机ID、监控数据时间、云主机内部IP地址、CPU使用率、内存使用率、普通存储使用率、高性能存储使用率、静态存储使用率、本地视频存储使用率、异地视频使用率、磁盘写峰值、磁盘读峰值、带宽上行峰值、带宽下行峰值
应用系统网络出口使用数据	信息系统编号、连接网络类型（政务外网/互联网）、监控数据时间、带宽上行峰值、带宽下行峰值
VPN/远程接入登录数据	信息系统编号、连接网络类型（政务外网/互联网）、监控数据时间、VPN远程接入类型（SL VPN/Ipsec VPN）、远程接入账号、会话ID、登入时间、退出时间
运维监测数据	运维监测类型（机房巡检、云平台运维、网络运维、安全运维）、监测内容、状态（是否正常）、监测时间、监测人
安全漏洞扫描数据	安全漏洞名称、漏洞类型（主机漏洞、数据库漏洞、WEB漏洞、中间件级其他组件漏洞等）、安全漏洞风险等级、漏洞存在的云主机ID、所属信息系统名称、扫描时间、漏洞通知情况（是否已联系系统责任人）、漏洞整改情况、漏洞整改时间
安全补丁安装数据	安全补丁名称、安装补丁的云主机ID、补丁类型（Windows补丁、Linux补丁、国产操作系统补丁、各类数据库补丁、中间件补丁）、安全补丁发布时间、安全补丁安装时间、监测人
安全预警监测数据	监测类型（漏洞发布/补丁发布）、监测内容、预警情况（是否已通知相关单位）、监测时间、监测人
安全攻击监测数据	安全攻击名称、攻击涉及云主机ID、攻击涉及信息系统编号、安全攻击通报情况（是否已通知相关单位）、监测时间、监测人