

团 体 标 准

T/DGAG 043—2026

政务云平台建设技术要求

Technical requirements for construction of government cloud platform

2026 - 04 - 02 发布

2026 - 04 - 15 实施

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 框架设计	2
5.1 技术框架	2
5.2 服务框架	3
6 技术要求	4
6.1 整体要求	4
6.2 机房环境要求	4
6.3 技术设施要求	5
6.4 支撑软件要求	7
6.5 业务应用要求	9
6.6 容灾备份要求	9
6.7 安全要求	10
6.8 云管平台与接口要求	10
6.9 多云协同要求	11
6.10 智能算力要求	12
6.11 其他要求	12
附录 A（资料性） 计算存储资源配置技术指标	14
A.1 虚拟机配置及技术指标	14
A.2 存储配置及技术指标	14
附录 B（资料性） 云平台数据汇聚规范（示例）	15
B.1 政务云平台监管数据汇集接口	15
B.2 资产数据	15
B.3 机房环控数据	16
B.4 日志数据	16
B.5 云平台数据	16
B.6 应用数据	16
B.7 监控数据	17
参考文献	18

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。

本文件由广州市数字政府运营中心、广州广电运通信息科技有限公司、广东数字政府研究院提出。
本文件由广东省数字政务协会归口。

本文件起草单位：广州市数字政府运营中心、广州广电运通信息科技有限公司、广东数字政府研究院、广东省数字政务协会、中国电信股份有限公司广州分公司、中国联合网络通信有限公司广州市分公司、腾讯云计算（北京）有限责任公司、广州市品高软件股份有限公司、江门市大数据管理中心、广州广宽科技有限公司、广州市数据要素产业协会、云浮市政务服务和数据管理局、梅州市政务大数据管理中心、茂名市信息中心、广东技术师范大学、广州市家盾卫士锁业有限公司、中国联合网络通信有限公司江门市分公司。

本文件主要起草人：吴鹏、刘愉滨、许阳光、付伟炳、张蔚铮、翁媛媛、邓盛威、吴文浩、张瑜、罗世荣、董耀艺、郑丹丹、曲舒琦、王川、萧翰霖、李莹、彭攀、马兴文、罗桦瀚、叶德智、张庆俐、陈苗、刘光明、徐雄鹰、黎良浩、周晓华、伍华新、沈成燕、林淡锋、薛松荃、黄国贤、陈倩婷、黄宜娇、李冬、黄俊凯。

政务云平台建设技术要求

1 范围

本文件给出了政务云平台整体技术要求，规定了政务云平台建设的机房环境要求、基础设施要求、支撑软件要求、业务应用要求、容灾备份要求、安全服务要求、运管平台与接口要求。

本文件适用于政务云管理部门、政务云使用单位、政务云资源服务商、政务云监管服务商及其他相关单位对政务云进行设计、规划、建设、验收等活动。

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—2023 信息安全技术 云计算服务安全能力要求
- GB/T 33780.1 基于云计算的电子政务公共平台技术规范 第1部分：系统架构
- GB/T 33780.2 基于云计算的电子政务公共平台技术规范 第2部分：功能和性能
- GB/T 33780.3 基于云计算的电子政务公共平台技术规范 第3部分：系统和数据接口
- GB/T 33780.4 基于云计算的电子政务公共平台技术规范 第4部分：操作系统
- 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 36326 信息技术 云计算 云服务运营通用要求
- GB/T 39786—2021 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

GB/T 34078.1—2017界定的以及下列术语和定义适用于本文件。

3.1

政务云平台 government cloud

运用云计算技术，为行政事业单位提供基础设施、支撑软件、应用系统、信息资源、运行保障和信息安全等服务的资源平台。

3.2

政务云管理部门 government cloud management unit

依据职责负责政务云的规划建设和运行管理的单位。

3.3

政务云使用单位 government cloud user

政务云服务的使用方。

3.4

政务云资源服务商 government cloud resource service provider
政务云服务的供应方。

3.5

政务云监管服务商 government cloud 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，是云计算服务监控、管理、分析和优化的重要工具，是支撑和保障的信息化架构。

4 缩略语

下列缩略语适用于本文件。

ARM: 进阶精简指令集机器 (Advanced RISC Machine)
BI: 商业智能 (Business Intelligence)
CPS: 每秒新建连接数 (Connections Per Second)
FC: 光纤通道 (Fibre Channel)
IOPS: 每秒的读写次数 (Input/Output Operations Per Second)
I/O: 输入输出 (Input/Output)
KVM: 基于内核的虚拟机 (Kernel-based Virtual Machine)
LUN: 逻辑单元号 (Logical Unit Number)
NAT: 网络地址转换 (Network Address Translation)
NFLOWI: 网络流量接口 (Network Flow Interface)
NPROTI: 网络协议接口 (Network Protocol Interface)
OWASP: 开放Web应用安全项目 (Open Web Application Security Project)
PUE: 能源使用效率 (Power Usage Effectiveness)
RDM: 存储裸设备映射 (Raw Device Mapping)
RDS: 关系型数据库服务 (Relational Database Service)
RPO: 恢复点目标 (Recovery Point Objective)
RTO: 恢复时间目标 (Recovery Time Objective)
SAN: 存储区域网络 (Storage Area Network)
SCSI: 小型计算机系统接口 (Small Computer System Interface)
SSD: 固态硬盘 (Solid State Drive)
SQL: 结构化查询语言 (Structured Query Language)
vCPU: 虚拟中央处理器 (Virtual Central Processing Unit)
VMI: 云主机接口 (Virtual Machine Interface)
VPC: 虚拟私有云 (Virtual Private Cloud)

5 框架设计

5.1 技术框架

政务云平台技术框架图如图1，由机房环境、基础设施层、支撑软件层、业务应用层、云管平台与接口组成，并在安全和灾备体系的保障下，为政务云使用单位提供统一服务支撑。



图1 政务云平台技术框架图

具体说明如下：

- 机房环境：为政务云提供安全、合规、完整的基础环境，包含供电系统、制冷系统、安防系统、智能监控系统等；
- 基础设施层：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；
- 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，保障业务稳定运行和敏捷迭代，包括但不限于容器、数据库服务、中间件服务以及操作系统服务等，并支持统一管理；
- 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，如云盘、BI 数据报表等；
- 容灾备份服务。为政务云提供本地数据备份和恢复的能力，支持数据级容灾服务，保障业务数据不丢失；
- 安全服务：为保障政务云全生命周期安全，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；
- 运管平台与接口要求：为政务云提供标准的接口，具备纳管相关物理设备及系统的能力。

5.2 服务框架

政务云平台服务框架图如图2，服务相关方由政务云管理部门、政务云使用单位、政务云监管服务商、政务云资源服务商组成，政务云资源服务商提供云服务目录，并根据服务等级协议提供符合质量要求的云服务资源。

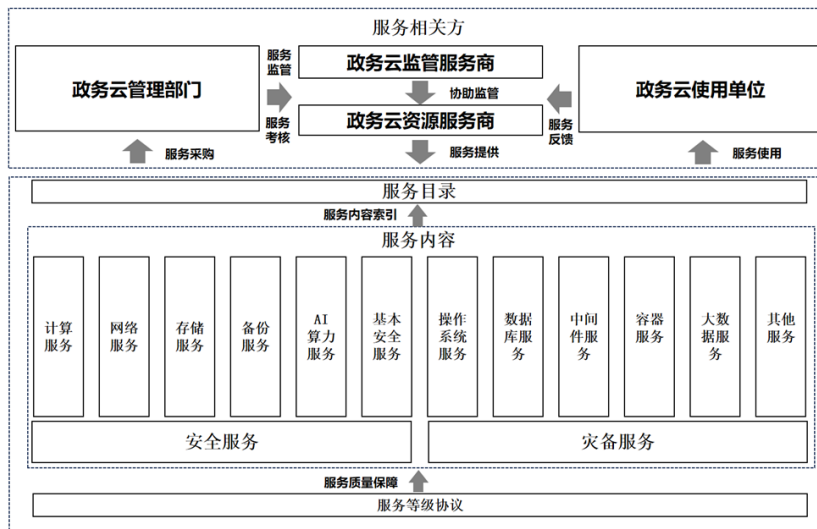


图2 政务云平台服务框架图

具体说明如下：

- a) 政务云管理部门牵头制定政务云的服务要求，采购云服务；负责政务云平台的服务监管与考核，并接受关于政务云服务的使用投诉；
- b) 政务云使用单位根据服务目录获得云平台资源服务，可就服务中的需求、问题向云服务商提出咨询或反馈；
- c) 政务云资源服务商根据服务目录提供政务云服务，响应使用单位的服务需求，接受政务云管理单位及政务云监管服务商的监管与考核；
- d) 政务云服务目录涵盖 IaaS、PaaS、SaaS、安全服务、灾备服务等内容；
- e) 政务云资源服务商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）为政务云使用单位提供服务；
- f) 政务云监管服务商在政务云管理部门的授权下，协助对政务云资源服务商的监督管理和考核。

6 技术要求

6.1 整体要求

政务云资源服务商提供的云平台应满足如下要求：

- a) 整体可用性¹⁾不低于 99.99%，数据可靠性²⁾不低于 99.9999%；
- b) 政务云全部设备，包括服务器、网络设备、存储设备、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，支持云平台整体的业务连续性³⁾目标不低于 99.99%。

6.2 机房环境要求

6.2.1 总体要求

总体要求如下：

- a) 应符合国家 A 级数据中心标准，新建机房应遵循 GB 50174—2017。
- b) 地址应位于本市行政范围内；
- c) 应配备建筑与结构系统、供电系统、制冷系统、安防系统、智能监控系统、网络与布线系统及消防系统；
- d) 宜具备为特殊用户需求划分独立物理区域的能力；

1) 可用性关注的是系统/服务能不能正常提供功能，以及正常运行的时间占比，针对的是系统的运行状态。

2) 可靠性关注的是数据本身的准确性、完整性、一致性，以及数据被正确读取/写入/存储的能力，针对的是数据的质量和可信用度。

3) 平台能够持续提供核心业务服务，或在服务中断后快速恢复核心服务，且不对用户业务造成实质性影响的能力。

- e) 机房有较好的容灾备份方案及措施，若某一地区发生不可抗力灾害，容灾机房能快速、有效承接原服务。

6.2.2 基本要求

基本要求如下：

- a) 新投产机房实际运行 PUE \leq 1.25，鼓励使用液冷、自然冷源、智能能效管控等低碳技术，优先采购绿色电力；
- b) 机房采用市电双回路供电，提高供电保障能力；
- c) 可用性应达到 99.9%；
- d) 宜设安防监控系统、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小于 3 个月；其他数据保存不小于 12 个月；
- e) 机房不得在居住场所或对外经营性场所楼内，且与最近的居住场所或大型经营性场所距离不小于 50 米；
- f) 同城异地容灾机房与主机房之间距离应保证不低于 20 公里，容灾机房与主机房之间应采用两路冗余光纤或专线进行互联，且容灾机房与生产机房不能处于同一供电站供电范围；非同城异地容灾机房选址应遵循 GB 50174 的要求。
- g) 机房具有 UPS 系统保障能力，UPS 电池满负荷放电时间不少于 30 分钟；
- h) 每机柜提供双路不间断供电，电力总功率每机柜不低于 3 千瓦。

6.3 技术设施要求

6.3.1 计算要求

6.3.1.1 计算资源要求

计算资源提供逻辑推理、数据处理、模型训练等能力，一般要求如下：

- a) 云主机应具备物理机的全部功能，如具有 CPU、存储、内存、网卡等资源，支持配置独立的 IP 地址、MAC 地址等网络标识；
- b) 宜支持 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) 应满足云主机之间、CPU 之间隔离保护要求；
- d) 宜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 I/O 等性能参数阈值进行动态调度；
- e) 宜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；
- f) 宜支持异构虚拟化能力，如 KVM、PowerVM 等多种虚拟化技术；
- g) 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；
- h) 宜支持虚拟机热迁移，可在不同代 CPU 资源池中进行虚拟机热迁移；
- i) 物理服务器 CPU 主频应不低于 2.0 GHz；
- j) 云主机可用性不低于 99.99%。

6.3.1.2 虚拟机技术指标要求

虚拟机技术指标一般要求如下：

- a) 计算资源宜按照 X86 架构和 ARM 架构提供不同规格的虚拟机，包括小型虚拟机、中型虚拟机、大型虚拟机等；
- b) 各种规格的虚拟机应明确 vCPU、内存、硬盘、CPU 主频、硬盘读写速度 IOPS 和网卡等配置（具体配置参见附录 A.1）；
- c) 虚拟机应支持提供单位 vCPU（1 核）和单位内存（1 GB）的定制化服务，以应对特殊业务场景资源需求。

6.3.1.3 裸金属技术指标要求

裸金属（指物理服务器）技术指标一般要求如下：

- a) 计算资源应按照 X86 架构和非 X86 架构提供不同规格的裸金属服务；

- b) 非 X86 架构宜包含 ARM、x86、LoongArch、SW64 等不同的指令集架构；
- c) 宜为裸金属服务提供可选配件，包括内存、磁盘、网卡、图形处理器（GPU）等，以应对特殊业务场景资源需求。

6.3.2 存储要求

6.3.2.1 存储资源要求

存储资源提供数据存储的能力，一般要求如下：

- a) 宜支持结构化数据、半结构化数据和非结构化数据等多种数据类型存储；
- b) 宜支持块存储、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) 宜支持存储资源扩展能力，例如支持扩展到 PB 级；
- 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，使用的密码算法应符合法律、法规的规定和密码相关国家标准、行业标准的有关要求；
- f) 存储系统的读写带宽应不低于 10 Gbps；
- g) 存储采用 SAN 或分布式存储架构，进行全路径冗余设计，存储服务全年可用率高于 99.99%；
- h) 应支持对存储空间的数据彻底销毁，对底层存储介质实现完全初始化，防止数据删除后被非法还原。

6.3.2.2 存储技术指标要求

存储技术指标一般要求如下：

- a) 存储资源应能提供多种存储服务，包括文件存储服务、FC-SAN 存储服务、IP-SAN 存储服务、对象存储服务、SSD 高性能存储服务等；
- b) 各种规格的存储服务应明确总体 IOPS、总体吞吐量、每客户端 IOPS、每客户端吞吐量等配置（具体配置参见附录 A.2）。

6.3.3 网络要求

6.3.3.1 网络系统要求

网络系统提供数据传输能力，一般要求如下：

- 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，应支持 IPv4/IPv6 双栈协议及无感转换能力，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) 宜采用双活网络架构，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；
- j) 云内骨干线路带宽不少于 10 Gbps；
- k) 服务器业务带宽不少于 10 Gbps；
- l) 平均可用性不少于 99.99%。

6.3.3.2 网络技术指标要求

网络技术指标一般要求如下：

- a) 网络系统要求：应能提供不同类型的网络服务，如硬件负载均衡、软件负载均衡等；

- b) 硬件负载均衡要求：10/100/1000 电口不少于 16 个，千兆光口不少于 4 个，万兆光口不少于 2 个；并发连接数不少于 1600 万；4 层 CPS \geq 50 万，7 层 CPS \geq 40 万，SSL CPS \geq 3 万；
- c) 软件级负载均衡要求：支持包含 TCP 和 UDP 的四层负载均衡，以及包含 HTTP 和 HTTPS 的七层负载均衡；支持对应用程序的健康状态检查。

6.3.4 托管技术指标要求

托管服务主要用于政务云使用单位将自行购置的服务器、网络设备、安全设备等专业设备托管放置在政务云资源服务商的机房内，由政务云使用单位自行维护的场景。政务云资源服务商提供上架、供电、供冷、政务外网链路、巡检（设备外观、指示灯、声音、振动等）等托管维护服务，一般要求如下：

- a) 网络服务的可用时间不少于 99.9%，电力供应的可用时间不少于 99.99%；
- b) 应提供共享 1000 Mb 电子政务外网网络，IP 地址由云管理平台分配；
- c) 上架开通时间不大于 5 小时（指设备入场及业务开通时间，不包含前期准备流程）；
- d) 应提供云平台内部管理网络的 KVM 远程管理功能；
- e) 应提供 7x24 在线技术支持。

6.4 支撑软件要求

6.4.1 数据库

6.4.1.1 总体要求

数据库为政务业务应用等提供数据存储能力，总体要求如下：

- a) 应支持关系型数据库及非关系型数据库；
- b) 关系型数据库宜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。

6.4.1.2 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，一般要求如下：

- 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) 宜支持多种资源部署模式，如裸金属、云主机、容器等；
 - 3) 宜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) 分析型数据库宜支持对时序数据进行存储和分析，宜支持标准云原生存算分离架构。
- c) 关系型数据库提供 RDS 单机版、HA 版、RAC 版三种类型，要求如下：
 - 1) 单机版采用单节点架构，无自动故障切换能力，服务器故障时业务会中断，需人工恢复，适用于非核心、测试及低可用要求场景；
 - 2) HA 版本使用一主一备的高可用架构，当主服务器故障时，实例会自动切换到备服务器运行；HA 主备版要求 RT0 \leq 30 秒，RPO \approx 0 秒；
 - 3) RAC 版本使用多节点的高可用并行架构，多个节点并行运行，任何单节点故障时，业务不受影响；RAC 版要求 RT0 \approx 0，RPO=0。

6.4.1.3 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数据库，一般要求如下：

- a) 应支持内存和硬盘的持久化存储方式；
- b) 宜支持多种资源模式部署，如云主机、裸金属、容器等；
- c) 宜支持虚拟网络，指定虚拟网络创建内存数据库实例；

- d) 宜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) 宜支持缓存服务的容灾。

6.4.2 中间件

中间件应满足应用支撑、消息通信、高可用及运维管理等相关技术要求。

6.4.2.1 应用服务器中间件

应用服务器中间件一般要求如下：

- a) 宜支持多服务器群集部署、负载均衡，支持对多种对象的集群功能；
- b) 宜支持热部署、远程部署等多种部署方式；
- c) 宜支持异构集群技术，当硬件平台或操作系统不是同一产品时，应用服务器能建立异构集群；
- d) 在业务系统不宕机的情况下，应支持动态增加服务器，扩充系统性能；
- e) 宜提供访问控制功能；
- f) 应提供审计功能，实现对用户在系统的事件进行记录和存储，能够进行查询，能够对审计进行响应。

6.4.2.2 消息中间件

消息中间件一般要求如下：

- a) 宜提供消息优先级控制功能、提供消息生命周期控制功能；
- b) 宜支持发送队列、本地队列、远程队列、虚拟队列等；
- c) 宜支持用户根据实际情况灵活组织节点，组建需要的网络结构；
- d) 宜支持常连接和按需连接两种模式，以更好地适应不同的网络通讯环境，节省系统资源和提高传输效率；
- e) 宜支持断点续传，消息保留在消息队列中，等待系统恢复后，消息将从传输失败点继续发送；
- f) 宜支持多种分发模式的集群，若干个节点组成一个群组，统一对外提供消息接收和处理功能，且集群内的各个节点对于应用是透明的；
- g) 应具有完整的日志功能，通过日志可以查看系统传输情况、消息的传输情况，并可以排除系统中出现错误信息。

6.4.3 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，一般要求如下：

- a) 应提供各类主流国产操作系统；
- b) 宜提供能适配不同 CPU 架构的操作系统，以适应不同业务应用需要；
- c) 宜具备拓展其他新型操作系统的能力；
- d) 宜保障操作系统使用的合法合规性与安全性。

6.4.4 容器

容器应满足资源管理、弹性伸缩、多环境适配及运维支撑等相关技术要求，一般要求如下：

- a) 应具备精细化管理能力，支持对 CPU、内存、存储、网络等资源的配额限制与使用率监控；
- b) 应提供资源分配与智能调度功能，支持统计容器及节点的资源利用率，并按照预设策略实现资源的动态分配与释放；
- c) 宜具备多租户管理能力，实现租户间资源隔离、权限独立及计量统计，满足政务不同部门的使用需求；
- d) 宜提供容器动态迁移功能，支持基于负载均衡的伸缩迁移、基于节点故障的容灾迁移，迁移过程中保障业务不中断；
- e) 宜支持容器镜像的上传、存储、共享与版本管理，支持将镜像授权给指定租户或用户使用；
- f) 应配套完善的运维系统、监控系统与日志系统，实现容器运行状态实时监测、异常告警及问题追溯。

6.5 业务应用要求

6.5.1 运行监测

运行监测服务解决用户业务系统间集成复杂、故障定位难、被动获取数据缺乏真实性等问题，实现辅助预警、态势感知、多系统间业务端到端调用过程回溯、划清责任边界的全面监控目标。一般要求如下：

- a) 支持探针自动发现，自动监控主机、进程、服务；
- b) 支持基于协议发现，自动梳理访问关系，形成应用、服务、业务拓扑，实现应用间复杂关系的可视化；
- c) 提供直观、易用的可视化界面，包括实时监控数据、历史数据分析、趋势分析等；
- d) 支持多维度、多视角的数据展示和分析，以全面了解业务系统的性能表现；
- e) 支持通过可视化及各类监控数据，对性能瓶颈进行分析排查，找出性能瓶颈或故障原因；
- f) 能够根据预设的警报阈值发送通知或警报。

6.5.2 网盘技术指标要求

网盘服务应满足文件管理、协作共享、安全存储及可靠备份等功能要求，一般要求如下：

- a) 网盘服务应包含多维度存储空间、多终端支持、同步盘功能、文件协作共享、文件快速迁移、数据摆渡、敏感内容检测、空间容量预警、文件历史版本管理、文档安全备份、多级权限管控、文件水印、数据脱敏处理等；
- b) 宜具备海量数据检索能力，能够提供多维度的检索，可以最大程度的处理数据的分析与检索；
- c) 宜支持一主一备的备份机制，保证各个区域保留多个副本保证数据一致与数据安全，当主库故障时，自动完成主从切换，避免单点故障，降低业务中断风险；
- d) 应提供不少于 2 副本方式保障数据安全，提升存储数据的完整性与安全性；
- e) 应提供离线备份能力，根据策略定期对系统数据和海量文件进行异地备份，备份过程不影响业务正常运行；
- f) 应支持存储加密，对网盘内存储的文件数据进行底层加密处理，采用独立密钥管理机制，实现文件数据加密存储与安全解密。

6.5.3 BI 数据技术指标要求

BI 数据服务应满足数据整合、分析展现、可视化及安全管控等要求，一般要求如下：

- a) BI 数据服务应提供多维分析和报表展现，快速获得分析结果；
- b) 宜支持多种数据源的集成，能够将不同数据源的数据汇总到一个仪表板中进行统一的分析；
- c) 宜支持多种数据可视化选项，如图表、图形和地图等，能够将数据以直观和易于理解的方式呈现给用户；
- d) 宜支持多用户的界面，使用户能够通过简单的拖放和筛选等方式轻松创建自定义报表和分析；
- e) 宜支持实时数据更新和分析；
- f) 应支持权限控制功能，确保只有授权用户才能访问敏感数据。

6.6 容灾备份要求

系统应建立完善的容灾备份体系，确保数据可靠、业务可恢复、运行可持续。

6.6.1 容灾技术指标要求

一般要求如下：

- a) 应提供同机房跨存储设备的数据容灾服务；
- b) 应提供实时同步、实时异步、分钟级定时保护策略；
- c) 当业务系统因故障停止服务时，应急接管并恢复业务小于 10 分钟，保障业务数据不丢失；
- d) 应急接管服务存储空间应与生产区业务系统所使用的存储资源池物理隔离；
- e) 应支持分布式数据库集群或业务集群的整体一致性恢复接管。

6.6.2 备份技术指标要求

一般要求如下：

- a) 备份介质本身具备高可用性和冗余性；
- b) 备份方式应包括完整备份、差异备份和增量备份；
- c) 备份服务全年可用率不小于 99.9%；
- d) 备份时不对数据库和文件的存取和写入造成很大性能影响，不能导致虚拟机、物理机低于最低指标；
- e) 备份恢复应以用户为单位做隔离，每个用户只能访问自己备份数据；
- f) 虚拟机镜像服务采用虚拟化层备份技术，无需在虚拟机中安装备份客户端，提供增量、差异、全量备份功能；
- g) 针对主流虚拟化平台，支持直接挂载备份集即可实现虚拟机的秒级恢复；
- h) 应实现同城异地备份，备份机房与生产机房距离不低于 20 公里，采用两路冗余光纤/专线互联，支持分钟级数据同步，RPO≤5 分钟；
- i) 宜部署跨地域异地备份，遵循 GB 50174 要求选址，与生产机房无共同地质、电力风险，采用加密传输，支持定时全量+增量备份，备份数据至少保留 6 个月，可快速异地恢复。

6.7 安全要求

政务云平台安全一般要求如下：

- a) 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—2021 中相应等级规定；
- d) 应保障云平台上的租户安全、容器安全、云主机安全、业务安全和数据安全；
- e) 云平台的安全服务宜包括虚拟防火墙、应用层防火墙、web 防篡改、主机漏洞检测、主机防病毒、数据库审计、日志审计、主机安全、网络安全等服务。

6.8 云管平台与接口要求

6.8.1 云管平台要求

政务云资源服务商应整合多个异构资源池，在资源池层面提供计算虚拟化、存储虚拟化、网络虚拟化等能力，在运营层面提供资源调度、资源监控、资源告警、高可用等能力，并开放 API 接口，满足以下基本技术要求：

- a) 支持虚拟机的生命周期管理，包括创建、删除、修改配置、查找搜索、快照、克隆等；
- b) 支持监控所接入的存储池的利用率监控，支持利用率阈值告警；
- c) 支持监控虚拟机、计算节点的 CPU、内存、存储使用率等指标，支持按照支持天/周/月/年维度展示；
- d) 支持监控数据保留不少于 1 年；
- e) 支持跨计算节点热迁移，支持跨存储迁移；
- f) 支持集群高可用，当某计算节点发生故障时，所承载的虚拟机能在其他计算节点重新启动，全程无需干预，要求 RTO 指标小于 10 分钟。

6.8.2 平台接口要求

6.8.2.1 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。

6.8.2.2 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) 硬件接入要求：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。

6.8.2.3 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 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。

6.9 多云协同要求

6.9.1 总体要求

总体要求如下：

- a) 应支持不同架构、不同厂商的异构云平台协同管理，实现资源统一纳管与调度；
- b) 宜具备跨云资源的标准化接入能力，兼容主流云平台接口规范，实现云资源的统一视图展示；
- c) 跨云业务调度应保障数据传输的安全性、一致性和低时延，满足政务业务连续性要求；
- d) 宜支持多云资源的弹性伸缩，根据业务负载实现跨云资源的动态分配与回收，整体调度响应时间不大于 5 分钟。

6.9.2 资源纳管要求

一般要求如下：

- a) 宜提供统一的多云管理门户，支持对异构云平台的计算、存储、网络资源进行统一监控、计量和计费；
- b) 宜支持主流云平台的虚拟化技术及接口标准，实现跨云主机、存储卷、虚拟网络等资源的生命周期管理；
- c) 宜具备跨云资源的拓扑可视化能力，展示异构云之间的资源关联、业务部署及数据流向；
- d) 宜对跨云资源的使用情况进行实时统计，支持按租户、业务系统、云平台维度进行资源使用率分析，数据更新频率不低于 5 分钟/次。

6.9.3 业务协同要求

一般要求如下：

- a) 宜支持跨云业务应用的无缝迁移，迁移过程中业务中断时间不大于 30 秒，数据无丢失；
- b) 宜具备跨云负载均衡能力，将政务业务流量智能分发至不同云平台的节点，提升业务整体可用性；
- c) 跨云部署的业务系统应支持统一的身份认证与权限管理，遵循政务云统一的安全认证规范；
- d) 应支持跨云业务的日志统一采集与审计，且跨云日志溯源可精准定位至操作节点。

6.9.4 数据协同要求

一般要求如下：

- e) 宜支持跨云数据的同步与共享，提供实时同步、定时同步等多种模式，同步数据一致性达到 99.9999%；
- f) 跨云数据传输应采用加密传输协议，符合商用密码应用安全性评估要求，防止数据传输过程中泄露、篡改；
- g) 应支持跨云数据备份与恢复，跨云备份数据可在任意对接云平台实现快速恢复，RTO≤10 分钟，RPO≈0。

6.10 智能算力要求

一般要求如下：

- a) 宜提供面向 AI 训练、AI 推理的智能算力资源，支持 GPU、NPU、AI 加速卡等异构算力硬件的虚拟化与池化管理；
- b) 智能算力池宜具备算力资源的弹性分配能力，支持按任务需求进行算力的快速调度与释放；
- c) 宜保障智能算力服务的高可用性，单算力节点故障时，任务可自动迁移至其他节点，任务中断时间不大于 1 分钟；
- d) 智能算力平台宜兼容主流的 AI 框架和开发环境，支持模型训练、推理部署、模型管理等全流程能力。

6.11 其他要求

6.11.1 扩展能力要求

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要求、政务云使用单位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。

6.11.1.1 云平台扩展要求

云平台扩展能力是指，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的能力，一般要求如下：

- a) 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；
- b) 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；
- c) 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；
- d) 应支持运维管理模块，包括租户和管理员门户、监控、报表等的按需开发，并支持自定义展示；
- e) 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。

6.11.1.2 系统对接扩展要求

系统对接扩展能力是指，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，一般要求如下：

- a) 应支持标准的 REST 风格 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、软件开发工具包（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) 制定规范性文件，根据以上三条 1)-3)，与第三方平台沟通确认后，制定接入规范性文件，政务云服务根据接入规范进行对接；
 - 5) 接入联调，按规范性文件，接入第三方服务，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。

6.11.2 监管数据汇集要求

6.11.2.1 概述

政务云资源服务商应在政务云管理部门的授权下，向政务云监管服务商提供汇集数据，用于开展监管工作。汇集数据应结合云管理单位的管理目标和内容进行详细定义，可通过政务云平台监管数据汇集接口进行数据汇集（相关示例参见附录B.1），汇聚数据范围包括资产数据（相关示例参见附录B.2）、

机房环控数据（相关示例参见附录B.3）、网络协议数据（相关示例参见附录B.4）、云平台数据（相关示例参见附录B.5）、应用数据（相关示例参见附录B.6）、监控数据（相关示例参见附录B.7）。

6.11.2.2 政务云平台监管数据汇集接口

政务云平台监管数据汇集接口按形式可分为NFLOWI、NPROTI、VMI和API共4种类型。获取运行监管信息和交付件的方式包括手工机制和自动机制。政务云监管服务商通过监管接口获取数据信息对政务云资源服务商进行持续监管，也可通过手工机制来实现。自动化机制的监管接口框架如图3所示。

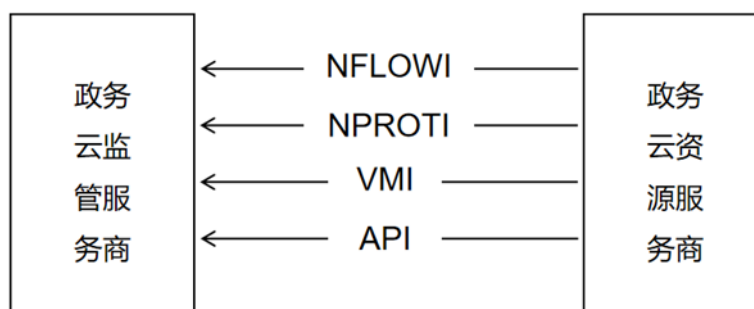


图3 政务云平台监管数据汇集接口框架图

6.11.2.3 监管数据范围

监管数据范围如下：

- a) 资产数据：包括但不限于物理环境资产、物理设备资产、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；
- b) 机房环控数据：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；
- c) 云平台数据：包括但不限于云平台规格数据、云平台网络接入 IP 数据等；
- d) 监控数据：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；
- e) 日志数据：包括但不限于安全设备日志和主机日志等。

附录 A
(资料性)
计算存储资源配置技术指标

A.1 虚拟机配置及技术指标

政务云平台虚拟机配置及技术指标如表A.1所示。

表A.1 政务云平台虚拟机配置及技术指标

虚拟机配置及技术指标	vCPU (个)	内存 (GB)	硬盘 (GB)	CPU主频 (GHz)	硬盘读写速度 (IOPS)	其他
小型虚拟机 (X86架构)	≥2	≥8	≥50	≥2.2	≥600	配置千兆网卡
小型虚拟机 (ARM架构)	≥2	≥4	≥100	≥2.0	≥600	配置千兆网卡
中型虚拟机 (X86架构)	≥4	≥16	≥100	≥2.2	≥600	配置千兆网卡
中型虚拟机 (ARM架构)	≥4	≥8	≥100	≥2.0	≥600	配置千兆网卡
大型虚拟机 (X86架构)	≥8	≥32	≥100	≥2.2	≥600	配置千兆网卡
大型虚拟机 (ARM架构)	≥8	≥16	≥100	≥2.0	≥600	配置千兆网卡

A.2 存储配置及技术指标

政务云平台存储配置及技术指标如表A.2所示。

表A.2 政务云平台存储配置及技术指标

存储配置及技术指标	总体 (IOPS)	总体吞吐量 (Mbps)	每客户端 (IOPS)	每客户端吞吐量 (MB/s)
文件存储服务	≥10000	≥3000	≥100	≥30
FC-SAN存储服务	≥50000	≥3000	≥800	≥180
IP-SAN存储服务	≥2000	≥3000	≥600	≥140
对象存储服务	≥15000	≥3000	≥600	≥100
SSD高性能存储服务	≥100000	≥3000	≥20000	≥350

附录 B
(资料性)
云平台数据汇聚规范（示例）

B.1 政务云平台监管数据汇集接口

政务云平台监管数据汇集接口如表B.1所示。

表 B.1 政务云平台监管数据汇集接口

云平台接口	接口分类	要求描述	数据汇集结果
网络流量接口 NFLOWI	物理网络接口	政务云资源服务商应向提供云计算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、审计云计算平台安全事件等综合监管工作	网络协议数据
	虚拟网络接口	政务云资源服务商应提供云计算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将指定流量根据指定策略牵引到政务云综合监管服务商的设备，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	政务云资源服务商应开启云计算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消息发送到云监管服务商的设备	日志数据
	SNMP接口	政务云资源服务商应开启云计算平台网络、安全设备的 SNMP协议管理接口，使得政务云综合监管服务商获取所有网络安全设备的运行信息	日志数据
	以太网接口	政务云资源服务商应为政务云综合监管服务商分配合适的以太网接口，保证云监管能监测到监管对象，政务云综合监管服务商可通过以太网口接入云计算平台网络，开展云平台安全监管工作	/
云主机接口VMI	云主机接口	政务云资源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	政务云资源服务商应根据综合监管工作的需要，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。（API接口依据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

B.2 资产数据

汇总云服务商云平台物理资产数据如表B.2所示。

表 B.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、虚拟机资产、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

B.3 机房环控数据

机房环控数据如表B.3所示。

表 B.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

B.4 日志数据

采集云平台物理网络中的安全设备日志、云主机日志数据，如表B.4所示。

表 B.4 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、安全设备代理 IP、安全设备名称、设备 S/N 号、设备类型、源 IP 及端口、目的 IP 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、操作系统类型、日志名称、日志类型、日志正文内容

B.5 云平台数据

政务云资源服务商提供云平台的整体管理数据，如表B.5所示。

表 B.5 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 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

B.6 应用数据

政务云资源服务商统计云平台入云信息系统的基本情况，如表B.6所示。

表 B.6 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、系统等级、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

表B.6 应用数据（续）

数据分类	数据内容描述
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、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、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、外网 IP、负载 IP、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 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 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

B.7 监控数据

向政务云监管单位提交云平台的管理数据如表B.7所示。

表 B.7 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（SSL 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、中间件及其他组件漏洞等）、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

参 考 文 献

- [1] DB11/T 2169—2023 政务云平台建设技术要求
 - [2] 中华人民共和国网络安全法
 - [3] 中华人民共和国数据安全法
 - [4] 中华人民共和国个人信息保护法
 - [5] 关键信息基础设施安全保护条例
 - [6] 政务数据共享条例
 - [7] 国务院关于在线政务服务的若干规定
 - [8] 广东省政务服务数字化条例
 - [9] 广东省公共数据管理办法
 - [10] 《国家政务信息化项目建设管理办法》（国办发〔2019〕57号）
 - [11] 《云计算综合标准化体系建设指南(2025版)》（工信部联科〔2025〕175号）
-