ICS 35.020
CCS L04

团 体 标 准

T/SDBDA 19—2021

电子政务云服务管理平台运维服务规范

E-government cloud service management platform operation and maintenance specification

2021－12－14 发布　　2021－12－14 实施

山东省大数据协会　　发 布

目　　次

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。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由山东亿云信息技术有限公司提出。

本文件由山东省大数据协会归口。

本文件起草单位：山东亿云信息技术有限公司、山东至信信息科技有限公司、山东聊云信息技术有限责任公司、山东旗帜信息有限公司、山东水发紫光大数据有限责任公司、青岛华睿互联科技有限责任公司、山东省数字证书认证管理有限公司、中孚安全技术有限公司、同智伟业软件股份有限公司、济南慧天云海信息技术有限公司、山东标准化协会、山东赛宝信息技术咨询有限公司、威海北洋云信息技术服务有限公司、泰山智能制造产业研究院、山东海湾软件科技有限公司、济南凡胜网络科技有限公司、山东省数字化应用科学研究院有限公司、青岛海纳云智能系统有限公司。

本文件主要起草人：李旋、胡峰、张记高、邱瀚、李勇、王伟、尚新、苗功勋、景年喜、张中华、郑霞、代振忠、张文龙、王丽、王风平、毕延洁、张吉良、崔为涛、鹿全礼、金岩。

电子政务云服务管理平台运维服务规范

1 范围

本文件规定了电子政务云服务管理平台运维服务的运维服务内容、运维服务保障、安全保障及应急服务等内容。

本文件适用于电子政务云服务管理平台的运维服务管理。

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 21061-2007 国家电子政务网络技术和运行管理规范

GB/T 22239-2019 信息安全技术网络安全等级保护基本要求

GB/T 28827.4-2019 信息技术服务运行维护 第4部分：数据中心服务要求

GB/T 34077.3-2021 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 34078.1-2017 基于云计算的电子政务公共平台总体规范 第1部分：术语和定义

GB/T 34080.1-2021 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 34080.2-2021 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 34080.4-2021 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

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

电子政务云服务管理平台 E-government cloud service management platform

运用云计算技术，统筹利用机房资源、计算资源、存储资源、网络资源、信息资源、应用支撑等资源，发挥云计算虚拟化、高可靠性、通用性、高可扩展性以及快速、按需、弹性的服务特征，为各政府部门构建提供基础设施、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电子政务综合性服务管理平台。

3.2

政务云 Administrative 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。

3.3

国家电子政务外网 National E-government extranet

国家电子政务外网是国家电子政务重要基础设施，是承载各级政务部门用于经济调节、市场监管、社会管理和公共服务等非涉及国家秘密的业务应用系统的政务公用网络。包括中央级政务外网和地方政务外网，二者均由相应的广域网和城域网构成。中央广域网与 31个省、直辖市、自治区和新疆生产建设兵团的省级政务外网互联。中央城域网用于连接在京中央政务部门，并与中央广域网高速互联。地方政务外网由省、地（市）和县级广域网和相应的城域网构成。

3.4

等级保护 Level Protection

根据网络在国家安全、经济建设、社会生活中的重要程度，以及其一旦遭到破坏、丧失功能或者数据被篡改、泄露、丢失、损毁后，对国家安全、社会秩序、公共利益以及相关公民、法人和其他组织的

合法权益的危害程度等因素，网络分为五个安全保护等级，这些相关工作定义为等级保护。随着新技术的发展,等级保护系列标准正在更新以适应新技术的发展,新的等级保护在本指南中统称为等级保护2.0。

4 运维服务内容

4.1 基础环境运维服务

4.1.1 机房运维管理应符合 GB/T 28827.4 的规定，还应遵循以下要求：

a) 建立巡检制度，运维人员应定期进入机房巡检，并做好记录；
b) 对机房相关设备进行监控，并提供事件或故障发生时的相应支持；
c) 提供优化改善服务，对机房的安全性及可靠性等级改善。

4.1.2 机房基础设施常规运维内容应符合 GB/T 28827.4 中的规定。

4.2 网络运维服务

4.2.1 网格运维管理应包括局域网、广域网、互联网、网络线路（包括专线、拨号网络、VPN）、路由器、交换机、防火墙、入侵检测、负载均衡、语音以及通信传输设备等。

4.2.2 网络运维管理应遵循 GB/T 21061 的规定，还应遵循以下要求：

a) 监控网络设备状态、网络连通性等运行状态；
b) 检查并保存网络设备运行日志；
c) 备份网络、防火墙、入侵检测等设备的配置参数；
d) 及时处理网络中断、网络设备故障；
e) 规划网络 IP 地址，提高互联网与政务外网 IP 地址利用率；
f) 配置政务外网与互联网网闸，实现安全跨网访问。

4.3 硬件平台运维服务

4.3.1 服务器运维服务

服务器运维服务应包括但不限于：

a) 应提供对服务器的整体运行情况、电源工作情况、CPU 工作情况、内存工作情况、硬盘工作情况、接口工作情况进行监控并做好工作记录；
b) 应提供对服务器的预防检查服务，包括：服务器的资源分配情况和策略、CPU 使用峰值情况、内存使用峰值情况、文件系统空间使用情况、网络情况等；
c) 应提供服务器运维过程中系统微码升级、配置文件备份、过期日志和文件系统清理、服务器硬盘配置检查、更换控制器电池、系统重启等服务；
d) 在服务器运维过程中，应提供事件驱动响应和服务请求响应等服务支持。

4.3.2 存储设备运维服务

存储设备运维服务应包括但不限于：

a) 应提供对存储设备的控制器工作情况、电源设备工作情况、数据存储介质工作情况、设备接口工作情况、存储设备介质空间使用情况、读写速率情况、读写命中率情况进行监控并做好工作记录；
b) 应提供对存储设备的预防检查服务，包括：存储速率情况、读、写缓存分配比例情况、数据读、写命中率情况、存储硬盘空间使用情况、存储系统日志情况、磁带池使用情况；
c) 应提供存储设备运维过程中系统微码升级、更换控制器电池、介质读、写正常性测试、配置文件备份、过期运行日志清理、链路端口访问测试等服务；
d) 在存储设备运维过程中，应提供事件驱动响应和服务请求响应等服务支持。

4.4 软件运维管理

软件运维服务应包括但不限于：

a） 问题报告单受理处理及反馈；
b） 软件版本的现场测试及升级；
c） 应用软件的重新部署；
d） 应用系统数据处理；
e） 突发事件响应及处理；
f） 应用软件维护；
g） 重要时间点的保障支持；
h） 以及各类外部数据交互程序维护。

5 运维服务保障

5.1 人员保障

5.1.1 应取得相应的技术能力等级认证，满足平台运维服务的需求。
5.1.2 应参加运维技术、业务、安全等培训，考核合格持证上岗。
5.1.3 应定期参与平台运维技术培训，确保技术与能力和平台相匹配。
5.1.4 熟悉平台使用方法、问题解决办法、使用规则等。

5.2 制度管理

5.2.1 应建立运维管理工作机制，制定运维管理制度，包括但不限于以下管理制度：
a） 机房管理制度；
b） 日常运维管理制度；
c） 运维过程管理制度。
5.2.2 应建立运维管理制度制定、发布、更新机制，定期修订和完善。

5.3 资产管理

5.3.1 应建立设备管理制度，明确到设备管理人，并建立制度的制定、发布、更新机制，定期修订和完善。
5.3.2 应在设备投入使用前对设备进行必要的验证性测试，并保留测试记录。
5.3.3 编制设备清单，内容至少包括设备名称、设备编号、购置时间、设备使用年限、设备主要参数、设备参数、设备状态、设备保修期、设备用途等。
5.3.4 设备应设专人管理，并对设备的状态进行监控和记录。

5.4 文档管理

5.4.1 应对运维服务过程中的记录性文档建立管理制度，并定期整理归档保存。
5.4.2 应建立文档管理制度，并设置专人进行管理。

6 安全保障

6.1 网络安全保障

网络安全管理应符合GB/T 22239-2019中8.1.10.6的规定，还应符合GB/T 34080.4以及以下要求：
a） 平台不承载高于其安全保护等级的业务系统；
b） 不同用户虚拟网络之间进行隔离；
c） 建立安全防护机制，对网络进行 24 小时监控，能检测到对客户发起的网络攻击行为，及时封禁攻击来源和记录攻击的类型、时间、流量并进行告警。

6.2 云资源安全保障

云资源安全管理应符合GB/T 34080.2的要求，还应符合以下要求：
a） 对于云资源的访问策略需要实行最小化原则，敏感端口需要指定访问源 IP；

b） 定期对云资源进行漏洞扫描，对于存在安全漏洞的云资源应及时告知用户，并协助用户处理。

6.3 数据安全保障

数据安全管理应符合GB/T 34080.1的要求，还应符合以下要求：

a） 提供快照服务、快照保护，防止快照中的数据被非法访问；
b） 云资源应具备多副本备份机制，并且各副本间的数据保持一致；
c） 提供数据迁移技术支持，保证用户数据迁移的安全、可靠。

6.4 运维安全保障

运维安全管理应符合GB/T 34077.3的要求，还应符合以下要求：

a） 建立安全运维制度，运维人员应在指定场所进行工作；
b） 运维人员账号应实行权限管理，定期修改账号密码；
c） 对运维专线使用进行管理，非运维人员不得使用运维网络。

7 应急服务

7.1 应建立应急处置机构，明确管理职责、管理内容、管理要求、处理流程等。

7.2 应建立突发事件预防预警处理机制，协助平台维护人员分析、处理突发事件，使平台在最短事件内恢复正常运行。

7.3 在突发事件处理完毕后，根据突发事件产生的原因，完成处理分析报告。在报告中应包含突发事件的描述、产生原因、解决办法、处理过程、责任人及后续的改进措施。

参 考 文 献

[1] GB/T 9361-2011 计算机场地安全要求
[2] GB/T 34080.3-2021 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