ICS 35.240.01
CCS L67

DB3713

临　沂　市　地　方　标　准

DB 3713/T 290—2023

市县级国土空间规划“一张图”平台运行环境建设规范

Specification of operating environment for‘Inteplan’ of urban and county-levelspatial planning

2023－08－22 发布　　2023－09－22 实施

临沂市市场监督管理局　　发布

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。

本文件由临沂市自然资源和规划局提出、归口并组织实施。

引　言

为规范临沂市及县级国土空间规划“一张图”平台运行环境的建设，搭建市县互联互通的云技术环境，基于《关于建立国土空间规划体系并监督实施的若干意见》（中发[2019]18号文）、《关于开展国土空间规划“一张图”建设和现状评估工作的通知》（自然资办发[2019]38号文）和临沂空间规划一张图建设实际，制定本文件。

市县级国土空间规划"一张图"平台运行环境建设规范

1 范围

本文件规定了市县级国土空间规划“一张图”平台运行环境的总体架构、中台要求和云租户要求。

本文件适用于临沂市的市县级国土空间规划“一张图”平台运行环境建设。

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 28827.1 信息技术服务 运行维护 第1部分：通用要求

3 术语和定义

下列术语和定义适用于本文件。

3.1 3.1

国土空间规划“一张图” ‘Inteplan’ ofspatialplanning

以基础地理信息和自然资源调查监测成果数据为基础，应用全国统一的测绘基准和测绘系统，集成整合国土空间规划编制和实施管理所需现状数据、各级各类国土空间规划成果数据和国土空间规划实施监督数据，形成的覆盖全域、动态更新、权威统一的国土空间规划数据资源体系。

[来源：GB/T 39972—2021，3.2]

3.2 3.2

国土空间规划“一张图”平台运行环境 operating environment for ‘Inteplan’ ofspatialplanning

支撑国土空间规划“一张图”平台构建的运行环境，包含硬件环境、软件环境、安全环境、运维环境。

3.3 3.3

云租户 cloud tenant

基于云技术的轻量级私有云，为用户提供计算、存储、网络服务能力，支持节点内和节点间网络管控及数据通讯等能力。

3.4 3.4

云捕捉 cloud observer

动态捕捉云租户节点信息，并进行各云租户节点的资源数据、监控数据、告警数据、性能数据的综合管理。

3.53.5

共享块 shared block

基于云租户内的共享文件块存储和同步传输，提供文件存储共享服务，满足用户在特定网络环境下文件跨平台的共享。

4 缩略语

下列缩略语适用于本文件。

API：应用编程接口（Application Programming Interface）

ACL：访问控制列表（Access Control List）

CI/CD：持续集成和持续交付（Continuous Integration/Continuous Delivery）

CVE：通用漏洞披露（Common Vulnerabilities & Exposures）

FTP：文件传输协议（File Transfer Protocol）

GIS：地理信息系统（Geographic Information System）

HDFS：Hadoop分布式文件系统（Hadoop Distributed File System）

IDE：集成开发环境（Integrated Development Environment） JWT：JSON网页令牌（Json web token）

KVM：键盘、视频和鼠标（Keyboard Video Mouse）

LDAP：轻型目录访问协议（Lightweight Directory Access Protocol）

MFA：多因子认证（Multi-factor authentication）

NAT：网络地址转换（Network Address Translation）

NFS：网络文件系统（Network File System）

SAML：安全断言标记语言（Security Assertion Markup Language）

SNMP：简单网络管理协议（Simple Network Management Protocol）

SPI：服务提供者接口（Service Provider Interface）

SSH：安全外壳协议（Secure Shell）

SSL：安全套接字协议（Secure Sockets Layer）

SSO：单点登录（Single Sign On）

UPS：不间断电源（Uninterruptible Power Supply）

VLAN：虚拟局域网（Virtual Local Area Network）

VNC：虚拟网络控制台（Virtual Network Console）

VPN：虚拟专用网（Virtual Private Network）

5 空间规划一张图平台运行环境总体架构

5.1 逻辑架构

架构拓扑图如图1所示。

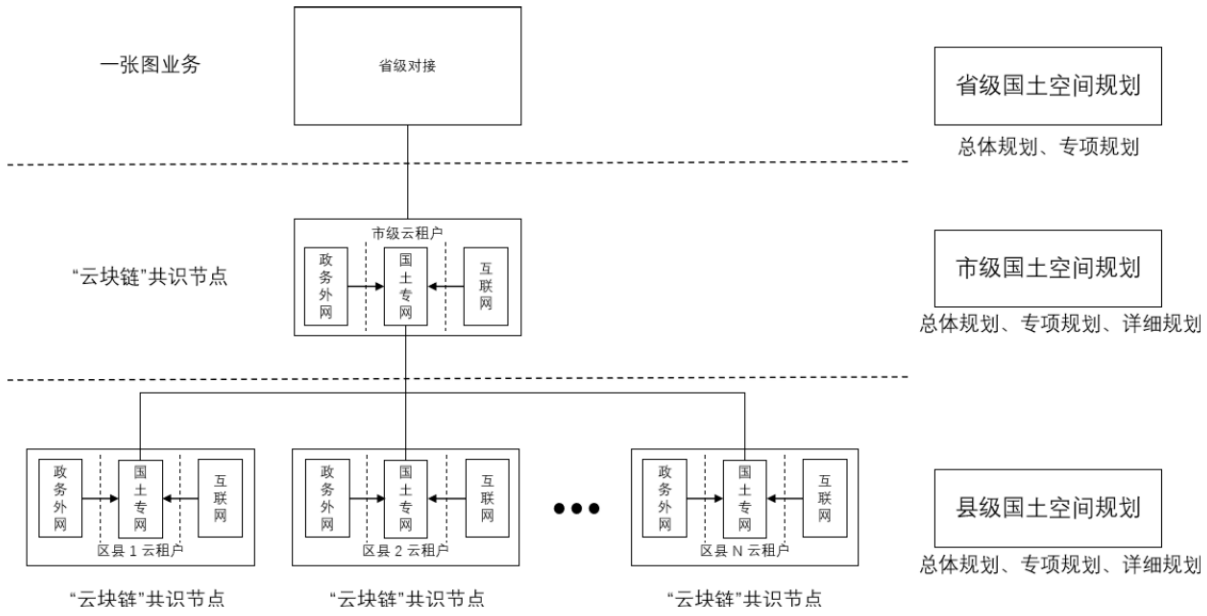

图1　省、市、县三级关系图

5.2　业务模型

业务模型应充分利用云计算、大数据技术，按照标准化、组件化的原则，建立分层实现的业务模型， 如图2所示。

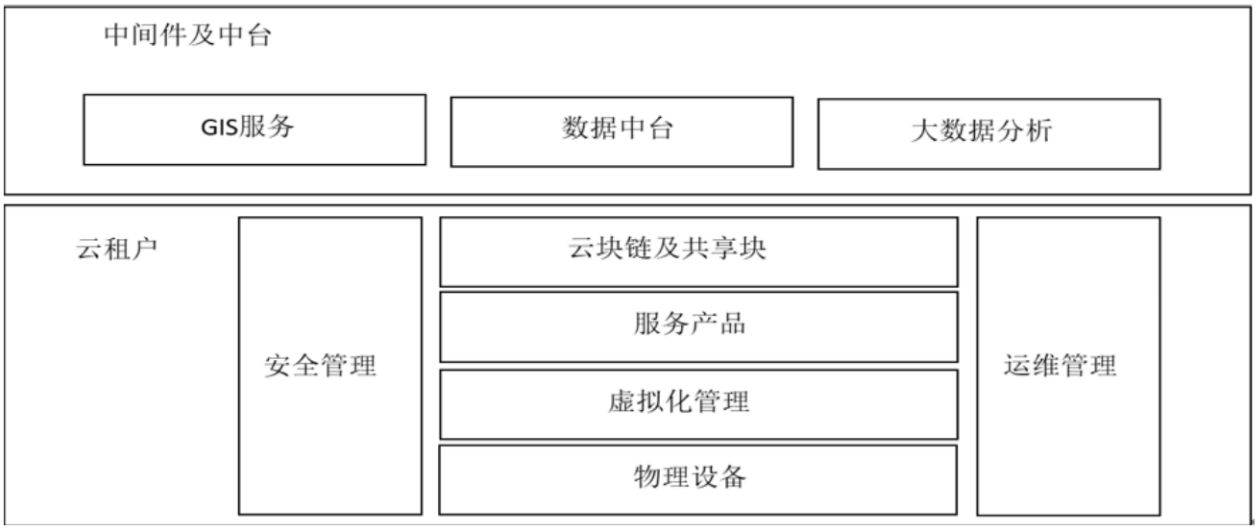

图2　业务支撑相关业务体系的分层模型

各层主要要求为：

a)　云租户：提供计算、存储、网络、安全、运维等一系列业务应用运行需要的 IT 资源及安全运行保护功能；

b)　中间件及中台：提供标准化组件及功能，供业务应用系统调用使用；

c)　业务应用：按照空间规划一张图的相关规范要求，建设实施并提供业务管理的支撑系统。

5.3 云块链节点与云租户

云块链为全市提供动态更新、权威统一、标准、可信任的空间管理支持能力。云块链架构主要包括市级云租户节点和各县级云租户节点，如图3所示。具体要求如下：

a) 云块链节点应基于可信数字身份，提供国土空间规划“一张图”信息平台一站式互联互通服务；
b) 云块链节点应具备灵活性和可扩展能力，宜支持异构；
c) 云块链管理应具备组件化设计和定义标准 SPI 的能力，宜根据不同业务场景或者同一业务场景中不同参与方的要求进行定制实现；
d) 云块链各构成节点的云租户设计应满足政务级应用的性能要求；
e) 各县级云租户应通过云捕捉按照标准接口信息管理注册为市级云租户的一个节点。

图3 云块链架构

5.4 云块链通讯与数据共享

具体要求如下：

a) 以市级云租户为中心建立星形云块链，按权限调控云租户之间的互联；
b) 县级云租户与市级云租户之间建立心跳机制，在失联时能够及时发出告警通知；
c) 提供云块链运行状态的图形化界面，显示注册、失联、连通等运行状态；
d) 建立连接的云租户间应可以实现数据通信，使用首部数据信息控制业务数据的传输。

6 中台

6.1 数据中台

数据中台通过建立一整套数据标准体系和数据处理规范，对多源、海量、异构数据进行采集、处理、存储、融合、治理，打通数据全生命周期关联，对数据进行深度分析与挖掘，充分发挥数据价值，并以服务方式对外输出各种数据能力，支持云租户内通过平台注册的各类应用系统提供数据调用服务，为优化各类业务办理和智能决策提供强有力的数据支撑。数据中台应满足如下功能：

a) 支持结构化、半结构化、非结构化数据的汇交与集成。
b) 支持可视化 ETL 建模，支持定时执行 ETL 模型；
c) 支持关系库、NoSQL 库、分布式文件系统、共享文件等数据存储方式；
d) 支持可视化数据开发，通过“拖拉拽”方式对数据处理过程进行建模设计；
e) 提供元数据管理，支持从数据库、ETL 模型、指标模型中自动抽取元数据；
f) 提供数据地图和数据血缘功能，实现数据全生命周期关联与表达；
g) 提供数据质检体系，支持自定义质检规则、质检模板和质检方案；
h) 支持免切片矢量数据快速显示，并支持动态数据服务；
i) 支持二三维空间数据一体化展示，并支持 BIM、CIM 数据展示；
j) 提供指标体系，统一指标分类、指标定义和统计口径；
k) 提供自助式 BI，支持柱图、饼图、折线图、仪表盘、地图、表格等数据可视化方式；
l) 提供 API 网关，实现服务注册、服务路由、服务授权与鉴权、服务监控、服务治理等功能。

6.2 GIS 云服务

云GIS将云计算的各种特征用于支撑地理空间信息服务，包括建模、存储、处理等，改变用户传统的GIS应用方法和建设模式。云GIS应满足如下功能：

a) 支持适配多种主流底层云平台；
b) 按需弹性资源调整，资源动态监测调整，满足应用层对 GIS 服务访问需求的变化，提升应用的稳定性和可扩展性；
c) 全方位的资源度量统计，提供资源使用情况统计和报表度量支持，可针对每个组织/用户使用云 GIS 平台资源的情况进行统计和报表度量；
d) 便捷的自服务方式，可以通过门户，以自服务的方式按需、快速的获取云 GIS 资源服务，减少了对 IT 部门的依赖，缩短了 GIS 资源的获取时间；

6.3 大数据分析

大数据分析通过聚合、回归、检测、聚类等手段，可视化、理解和处理大数据，洞察可能隐藏在数据中的模式、趋势和异常等。大数据分析应满足如下功能：

a) 提供多源数据接入能力；
b) 提供高效的大数据分析能力；
c) 提供简单便捷的产品化部署能力；
d) 提供实时动态的任务监控能力；
e) 支持把大数据分析结果输出到文件；
f) 提供灵活的系统部署方式。

7 云租户

7.1 云租户结构

7.1.1 云租户采用“平台+服务”的设计，根据临沂市/县空间等级进行逻辑分层，基于云平台专有网

络，支持总控中心（市）与分控中心（县）的双向数据传输，云租户功能架构如图 4 所示。

图4　云租户功能架构

7.1.2　核心层次要求如下：

a)　硬件设备：标准的通用设备，主要有服务器、交换机等；

b)　虚拟化管理：在硬件设备的基础上，通过虚拟化技术，实现计算、存储、网络资源的软件化定义和管理；

c)　服务产品：基于虚拟化技术实现的计算、存储、网络等 IT 资源，供租户使用的云资源；

d)　通讯及对接：在云租户里负责实现云租户间互联互通对接，以及云租户内部不同应用系统间的业务数据传输；

e)　安全管理：确保运行在云租户上的业务应用系统具有安全保护，并能支持通过等保三级的安全要求；

f)　运维管理：使业务系统、云租户能正常运行而设置的各种支撑工具。

7.2　虚拟化平台

虚拟化平台是云租户中的核心模块，关键功能要求如下：

a)　提供抽象化物理硬件形成计算、存储和网络资源池，通过统一管理和调度为上层服务提供计算、存储、网络资源，满足业务的动态变更、资源的智能管理和服务的自动化交付；

b)　平台提供丰富的南北向接口，符合 RESTful API 标准，供平台服务产品或合作伙伴调用使用，实现定制化需求；

c)　支持对资源池宿主机进行管理，支持宿主机关闭服务功能，支持对已关闭的宿主机上的虚拟机进行疏散；支持配置存储、计算等池化的调整及配置；

d)　支持虚拟机创建均衡分布算法和亲和性策略，能够实现不同物理主机分布扩展虚拟机；

e)　支持空间规划“一张图”云块链的网络特性、部署及集成要求。

7.3　云服务产品

7.3.1　云服务器

云服务器是一种简单高效、安全可靠、处理能力可弹性伸缩的计算服务，其管理方式比物理服务器更简单高效。通过公共镜像和私有镜像创建指定存储类型的系统盘，并且可以基于卷进行云服务器整

机备份，需要时进行恢复。云服务器应满足如下功能：

a) 支持多种云服务器规格，创建完成后可以根据需要进行规格变更；
b) 支持多种存储类型，包括 SATA 盘、SSD 盘等；
c) 支持多种镜像类型，包括公共镜像或私有镜像。公共镜像支持多种 Linux 及 Windows 操作系统类型；
d) 支持多种云服务器管理方式。云服务器应提供基于 Web 的用户界面，支持对云服务器实例进行启动、调整配置、重置系统等操作。提供 API 的访问方式，支持用于第三方的二次开发或集成；
e) 支持多种登录方式。包括密码登录、密钥登录、VNC 登录；
f) 支持多维度安全防护。支持关联多个安全组，进行安全组规则保护，为不同的云服务器实例设定不同的防火墙；
g) 支持可靠的数据服务。支持云服务器备份，并可根据备份进行恢复。数据存储提供三副本专业存储策略，消除单点故障，保证数据可靠性。

7.3.2 云硬盘

云硬盘为云服务器提供高可用、弹性、高性能、低时延的数据块级随机存储，云硬盘底层支持分布式存储和集中式存储两种存储架构，支持对挂载到云服务器上的云硬盘做格式化、创建文件系统等操作， 并提供数据持久化存储。云硬盘应满足如下功能：

a) 支持多副本。云硬盘采用多副本，业务数据以多副本的形式分布存储在块存储集群中，保证读写过程的稳定性，无单点故障；
b) 支持多种规格。如 SATA 盘、SSD 盘等；
c) 支持备份。支持手动和自动备份，自动快照功能提供对云硬盘数据的定时备份，可进行回滚操作以恢复云硬盘数据，提供高可靠的数据存储。支持增量备份，有效节省存储空间和备份时间；
d) 支持容量扩展。支持对云硬盘进行扩容，支持多个云硬盘挂载到同一云服务器，实现对海量数据的存储能力。

7.3.3 负载均衡

负载均衡可以对多台云服务器进行流量分发，提升系统整体的服务能力，消除单点故障。提供一种廉价有效透明的方法扩展网络设备和服务器的带宽、增加吞吐量、加强网络数据处理能力、提高网络的灵活性和可用性。负载均衡应满足如下功能：

a) 支持高访问量的业务；
b) 支持扩展应用程序；
c) 支持消除单点故障。

7.3.4 云缓存

云缓存是一种基于内存的高性能、高可用的键值对（Key-Value）内存缓存服务，其主要用途在于缓解后端数据库及存储服务的压力、快速响应热点数据等。云缓存应满足如下功能：

a) 实例管理：支持多样的实例管理功能，包括遍历实例列表，配置列表展示字段，根据 IP，ID 等搜索实例，展示实例详情内容，重启实例操作，修改实例名称，更换实例绑定安全组，重新配置实例密码，修改可维护时间段等；
b) 参数配置：支持修改实例参数，记录参数修改历史；
c) 实例监控：支持多项监控信息展示，支持手动及自动刷新监控数据，支持调整展示监控项，调整监控项展示顺序；
d) 备份恢复：支持手动/自动备份，提供自动备份策略配置；支持使用备份对实例进行恢复。

7.3.5 云物理主机

云物理主机提供高性能、无虚拟化、安全隔离的物理服务器集群，满足核心应用对高性能及稳定性的需求。云物理主机应满足如下功能：

a) 支持高性能计算能力：采用高规格硬件配置与高 I/O 设备的专属云物理主机，提供无虚拟损耗的计算性能，满足客户对高性能应用场景的需求；
b) 支持多场景：支持多种型号不同规格的物理机配置，不同类型的实例在 CPU、内存容量、存储介质、存储容量、网卡数量等维度有不同的配置，适用于不同业务场景；
c) 支持快速灵活部署。

7.3.6 虚拟私有网络

虚拟私有网络是基于云平台构建的云上虚拟网络环境，为用户提供安全隔离的私有资源部署平台，用户可自行规划 IP 地址范围及网段，配置安全组、网络 ACL、路由表，实现对私有网络的全方位管理。虚拟私有网络应满足如下功能：

a) 支持软件定义的方式管理私有网络，实现 VPC、子网网段规划；
b) 支持路由表管理，与 VPC 联动创建，并自动关联路由表；
c) 支持安全组管理，支持灵活的自定义访问规则；
d) 支持子网粒度的访问控制，可为用户提供子网级的网络 ACL 控制，可控制出入整个子网的流量，提供更加细粒度子网级的防护；
e) 支持提供对等连接方式，使用私有 IP 地址在两个VPC 之间进行通信；
f) 互联互通，提供弹性公网 IP、负载均衡、NAT 网关等多种方式连接公网。

7.3.7 弹性公网 IP

弹性公网IP可灵活的与各种云资源进行绑定和解绑，实现云资源的自由漂移。弹性公网IP应满足如下功能：

a) 支持与多种云资源绑定、解绑。可将弹性公网 IP 应用到任何一台云服务器/负载均衡器上；
b) 支持加入共享带宽的能力,支持独享一条带宽和加入共享带宽，通过共享带宽降低使用成本；
c) 支持流量统计及监控功能,支持实时统计及监控弹性公网 IP 的带宽使用情况，支持用户对业务流量波动情况的完整追溯。

7.4 运维监控

7.4.1 运维监控分为多源采集、传输/处理、存储/查询、展现/接口四部分。采集范围包含服务器、网络设备、存储设备、平台系统、平台组件、容器，以及各个平台业务的性能指标数据，并可分级处理各集群的数据，采用增量传输机制，有效降低数据传输压力。运维监控应满足如下要求：

a) 应提供对新服务和设备的识别、接入、纳管和监控等功能；
b) 应提供多种类型和资源的监控，如基础设施，通用中间件，微服务，应用等；
c) 提供 WEB 页面，提供友好的 web ui，并提供图表定制，dashboard 定制功能。

7.4.2 运维监控架构如图 5 所示。

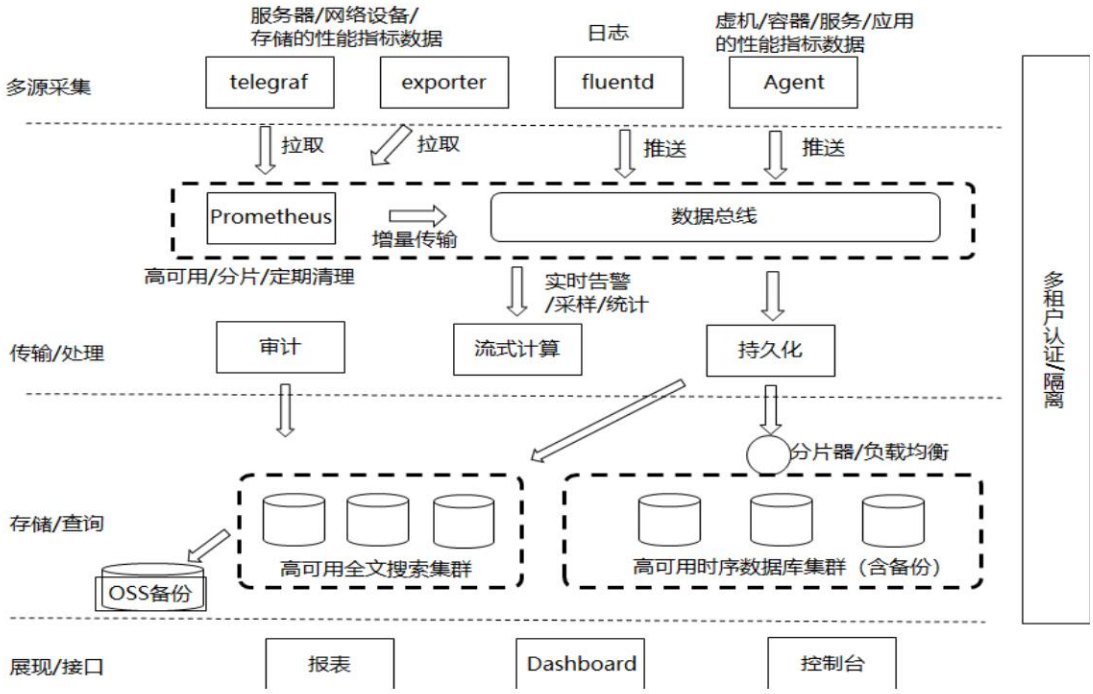

图5　运维监控功能结构

7.5　共享块

共享块用于云租户内的应用系统之间的数据共享传输。共享块基于哈希算法，实现文件传输过程的断点续传确保数据传输的稳定性和完整性；采用内存方式提高过程数据交互速度，用以应对云租户内复杂的文件共享关系及共享消费链路追踪，通过解析并记录文件，以报表形式分析共享效率。共享块应满足如下功能：

a)　支持不同类型的文件数据传输，在传输过程中，可实时查看文件数据的传输状态；
b)　支持文件数据的断点续传、读写过程控制、状态监控、权限隔离等功能；
c)　支持数据文件和头文件配对机制，实现传输过程管控功能；
d)　支持传输过程、各环节状态可视化展示功能；
e)　支持传输通道专用机制，并通过 1 进2 出的模式控制同通道的传输生命周期管理；
f)　支持文件数据的生命周期管理，包括排队，上传、下载、清除、管理等。

7.6　鉴权

7.6.1　身份认证

统一认证和授权，提供身份认证和权限分配、访问控制等功能的管理服务，管理用户（比如员工、系统或应用程序）账号用户资源的操作权限。帮助用户控制敏感信息，避免用户的账号密码或密钥的权限过大。通过用户维度的资源隔离，降低误操作风险，提高资源管理效率。身份认证应满足如下功能：

a)　开发和运维身份认证：提供租户控制台和管理员控制台；支持用户管理和权限管理；支持平台运维管理；
b)　鉴权：提供统一认证、统一授权、统一鉴权功能；提供用户管理、用户组管理、权限元数据管理功能；提供 SSO 单点登录和委托功能；
c)　应用集成：提供 OpenAPI、SDK、Adapter 方便外部应用集成；支持 OIDC、SAML2 等标准单点登录协议，可以实现与外部应用的无缝对接；支持 LDAP 目录协议。

7.6.2 授权管理

根据用户角色的不同为用户赋予各功能的权限。授权管理应满足如下功能：

a) 标准协议无缝集成：支持标准 OIDC 协议和 SAML2 协议，可以与支持该协议的外部应用无缝对接；
b) 支持标准身份凭证 JWT：凭借 JWT 调用服务接口，服务应用可直接从 JWT 中获取用户信息，而无需频繁与认证授权中心交互；
c) 提供基于策略的细粒度权限控制：支持资源实例级别的授权，精准控制功能权限和数据权限；
d) 支持为用户和用户组（角色）授权：支持为用户授权、用户组授权，用户加入用户组后自动拥有该用户组所关联的权限；
e) 支持为服务授权：支持为服务授权，用户可以授权某些云服务访问自己账号下的资源；
f) 支持签名认证请求：支持签名认证，用户可以凭借使用自己的私钥签名请求，进行云资源的访问，保证数据传输的安全性；
g) 支持 MFA 两步认证；
h) 完善的系统安全策略：密码强度限制、密码强制定时更新、登录日志、登录白名单、防暴力破解、关键 Cookie HttpOnly、密码加盐不可逆加密存储。

7.7 云捕捉

云捕捉用于云租户云节点捕捉，同时可用于资源数据、监控数据、告警数据、性能数据的综合管理。云捕捉应满足如下功能：

a) 支持对云服务器、负载均衡实例、云物理主机、CPU、磁盘读写、网络性能等数据的监控审查；
b) 支持资源告警，将计算资源、网络资源、存储资源进行合理规划与管控；
c) 支持云租户实例的注册、连接、健康检查、心跳检测等功能。

7.8 云部署

云部署是指通过云租户捕捉系统建立通讯机制，在云租户内检查云租户提供的计算、存储、交换等各种资源对平台应用系统的支撑能力，通过远端部署以云租户为单位部署各类空间规划一张图应用系统，并实现按版本更新。云部署应满足如下功能：

a) 支持从基础设施、虚拟化、分布式存储、数据库、各应用中间件的自动检索与检查的全栈云自动化快速部署；
b) 支持同时往多个云租户进行部署；
c) 支持以版本的方式对应用系统进行管理，通过版本迭代实现系统部署更新。

7.9 设施设备

7.9.1 机房要求

机房要求见表1。

表1 机房要求

主要项目	关键指标的目标值
基本要求	1.机柜数量：不宜低于机柜数×5（个） 2.单机柜功率：不宜低于3KW 3.机柜尺寸：1200mm×600mm×2000mm（长、宽、高），42U标准机柜 4.PDU要求：双路PDU，每个PDU输出接口不宜小于18个

表 1　机房要求（续）

主要项目	关键指标的目标值
供电电源	宜采用2路市电或1路市电+柴发（不应选址在频繁停电地区）
变压器	宜采用(N+1)/2N架构
UPS	宜采用2N冗余
空调	宜采用N+1架构
其它	1.提供监控室，监控到工位 2.提供基础环境及配套设施7×24h运维支持

7.9.2　设备要求

硬件设备包括网络设备、安全设备、主机设备、存储设备等；软件设备可分为操作系统软件、平台软件、安全软件等。基于国土空间规划“一张图”的系统建设要求，最低设备标准见表 2。

表2　设备要求

序号	设备名称	单位	数量
1	网闸	台	1
2	超融合物理节点	台	3
3	业务核心交换机	台	2
4	综合安全接入网关	套	2
5	辅材	套	1
6	裸金属物理节点	台	1-3
7	防 DDoS（互联网）	套	2
8	WAF（互联网）	套	2
9	轻量版私有云平台	套	1
10	共享块	套	1
11	主机安全	套	10
12	杀毒软件	套	10
13	堡垒机	套	1
14	日志审计	套	1
15	漏洞扫描	套	1

7.10　安全运维

7.10.1　安全要求

国土空间规划“一张图”的系统建设和运行维护应建立由物理安全、网络安全、数据安全、系统安全等构成的安全保障体系；明确各类数据的安全属性，杜绝并积极消除信息交换和信息共享存在的安全风险，强化边界保护措施，加强保密防范技术投入，切实做到“人防、物防、技防”相结合。

运行环境需按照网络安全等级保护 2.0 规范，符合三级标准要求。

7.10.2　运维要求

运行维护应符合GB/T 28827.1的要求，并在政策机制及人员组织等方面进行保障，包括:

a)　制定软硬件环境维护机制相关规范，包含机房要求、硬件维护要求和软件要求等；

b)　制定系统运行维护机制相关规范，包含运行管理规定、维护操作规定等；

c)　建立专业、稳定的技术支持团队。

参 考 文 献

[1] GB/T 34982　云计算数据中心基本要求

[2] GB/T 39972　国土空间规划“一张图”实施监督信息系统技术规范

[3] GB/T 51399　云计算基础设施工程技术标准

[4] 国务院.关于建立国土空间规划体系并监督实施的若干意见.中发〔2019〕18号,2019.

[5] 自然资源部办公厅.关于开展国土空间规划“一张图”建设和现状评估工作的通知.自然资办发〔2019〕38号,2019.

[6] 自然资源部办公厅.关于加强国土空间规划监督管理的通知.自然资办发〔2020〕27号,2020

[7] 国土资源部,国家测绘地理信息局.关于推进国土空间基础信息平台建设的通知.国土资发〔2017〕83号,2017