

T/JXEA

江西省工程师联合会团体标准

T/JXEA-364-2026

云计算多云管理平台互联互通技术要求

Technical requirements for interconnection and interoperability of cloud computing multi-cloud management platforms

（征求意见稿）

2026—XX—XX 发布

2026—XX—XX 实施

江西省工程师联合会 发布

目 次

前 言 II

引 言 III

1 范围 1

2 规范性引用文件 1

3 术语和定义 1

4 总则 2

5 平台互联互通基础架构要求 2

6 核心互联互通技术要求 3

7 互联互通安全技术要求 3

8 互联互通性能与可靠性要求 4

9 互联互通测试与验证 4

10 运维与服务管理要求 5

前 言

本文件依据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。

本文件由内蒙古自治区达拉特旗气象局提出。

本文件由江西省工程师联合会归口。

本文件起草单位：

本文件主要起草人：

引 言

随着云计算技术的广泛应用，企业及组织普遍采用多云部署策略以规避单一厂商锁定、优化成本与性能。然而，不同云平台之间的架构异构、接口差异及数据孤岛问题，导致多云管理面临资源难统管、数据难流动、业务难协同等突出挑战。为规范多云管理平台的互联互通能力，打破技术壁垒，实现跨云资源的统一纳管、数据的顺畅流动、业务的协同调度及安全策略的统一管控，特制定本文件。本文件规定了多云管理平台互联互通的基础架构、核心技术要求、安全要求、性能与可靠性要求、测试验证及运维管理规范，旨在为平台研发、部署、运营及测评提供技术依据，推动云计算产业生态的开放协同与高质量发展。

云计算多云管理平台互联互通技术要求

1 范围

本规范规定了云计算多云管理平台开展互联互通建设、运行及维护的通用技术要求、管理规范与测评方法。本规范适用于面向企业、政府及各类组织提供多云管理服务的平台，涵盖公有云、私有云、混合云等多种云形态的跨平台互联互通，包括但不限于云资源纳管、跨云数据流动、资源统一调度、业务跨云部署、安全策略统一管控、运维监控协同等场景的技术实现。

本规范适用于多云管理平台的研发厂商、部署实施方、运营服务方及第三方测评机构，云服务商提供的原生云管理平台如需实现跨云互联互通功能，可参照本规范执行；面向特殊行业（如金融、电力、医疗）的多云管理平台，在满足本规范基础上，还应符合行业专属的技术与安全要求。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，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。

GB/T 32400 信息技术 云计算 参考架构

GB/T 35295 信息技术 云计算 大数据融合架构要求

GB/T 38636 信息技术 云计算 平台即服务（PaaS）安全要求

GB/T 40657 信息技术 云计算 多云管理平台技术要求

YD/T 3986 算力互联互通能力要求 第1部分：总体要求

YD/T 4099 算力互联互通能力要求 第4部分：数据流动

3 术语和定义

3.1

多云管理平台 multi-cloud management platform

具备对多个云服务商的计算、存储、网络、数据库等云资源进行统一纳管、调度、监控、运维的云计算管理平台，是实现跨云互联互通的核心载体。

3.2

平台互联互通 platform interconnection and interoperability

指多云管理平台与各云服务商平台、平台内部各功能模块、以及多云管理平台与企业业务系统之间，实现资源信息、业务数据、管控指令的标准化交互，以及跨云资源、数据、业务的协同调度与运行的能力。

3.3

接口归一化 interface normalization

指多云管理平台对不同云服务商的异构API接口进行封装、适配，形成统一的标准化接口体系，屏蔽云厂商的接口技术差异，实现跨云接口的统一调用与管理。

3.4

数据归一化 data normalization

指多云管理平台对各云平台的资源数据、业务数据、运维数据等进行标准化格式定义与映射，实现跨云数据的结构统一、语义一致，保障数据的跨平台流通与共享。

3.5

跨云资源调度 cross-cloud resource scheduling

指多云管理平台基于互联互通能力，根据业务需求、资源负载、成本等因素，对分布在不同云平台的计算、存储、网络等资源进行统一分配、弹性伸缩与调度优化的过程。

3.6

算力互联互通 computing power interconnection and interoperability

指多云管理平台实现不同云平台算力资源的统一感知、调度与协同使用，支持算力跨云按需分配、弹性流转的能力。

3.7**配置漂移 configuration drift**

指多云管理平台纳管的跨云资源配置，因人工操作、云平台自身更新等原因，偏离预设的标准化配置基线的现象。

3.8**跨云数据流动 cross-cloud data flow**

指在多云管理平台的管控下，业务数据、资源数据在不同云平台之间的安全、高效传输、同步与共享，包括数据备份、迁移、同步等场景。

4 总则

多云管理平台的建设方、运营方是平台互联互通工作的责任主体，应建立健全互联互通技术管理体系，配备相应的技术研发、部署实施、运维保障团队，确保互联互通技术要求落地到位。平台互联互通应遵循标准统一、安全可控、高效协同、可扩展兼容的基本原则。

必须根据企业多云部署的实际需求、云资源类型、业务场景特点，科学设计互联互通架构，动态优化技术方案；应采用国家、行业通用的技术标准与接口规范，优先选择兼容性强、开放性高的技术架构，避免技术壁垒；在实现互联互通的同时，应将安全保障贯穿于设计、开发、部署、运行全流程，确保跨云资源、数据、业务的安全；应具备良好的可扩展性，支持新增云服务商、云资源类型及业务场景的快速适配；所有参与平台互联互通建设、运维的技术人员应接受专业培训，掌握标准化接口、数据归一化、跨云调度等核心技术要求，考核合格后方可上岗。

5 平台互联互通基础架构要求**5.1 架构整体要求**

多云管理平台互联互通架构应采用分层解耦的微服务架构，具备接入层、归一化层、核心服务层、应用层的四层架构体系，各层之间通过标准化接口实现数据与指令的交互，层内模块具备高内聚、低耦合的特性，支持独立部署、升级与扩展。架构应支持多租户隔离机制，确保不同租户的互联互通数据与操作相互独立，满足企业级数据隔离需求（来源：GB/T 32400，5.1）。

5.2 各层技术要求

接入层：作为多云管理平台与各云服务商平台、企业业务系统的连接入口，应支持主流云服务商的原生API接口、SDK及通用网络协议（HTTP/HTTPS、WebSocket等），具备高并发接入能力，支持新增云服务商的快速接入配置；应配置接入代理节点，实现对各云平台接入请求的转发、限流与监控，保障接入过程的稳定性。

归一化层：是实现互联互通的核心基础层，应具备接口归一化、数据归一化、权限归一化三大核心能力。接口归一化需封装形成统一的抽象接口体系，支持对云厂商API版本差异的屏蔽；数据归一化需定义通用的资源数据、业务数据模型，实现各云平台异构数据的格式映射与语义统一；权限归一化需基于RBAC模型，将各云厂商的IAM权限体系转化为平台统一的权限矩阵，支持细粒度的跨云权限管控。

核心服务层：应包含资源纳管、数据流动、资源调度、安全管控、运维监控等核心服务模块，各模块通过标准化的服务接口实现协同联动；应配置工作流引擎，支持跨云互联互通场景的流程自动化编排，如跨云资源弹性伸缩、数据自动备份、故障跨云迁移等。

应用层：应面向用户提供可视化的互联互通操作界面，支持跨云资源的统一展示、跨云数据的流动配置、跨云业务的部署调度等功能；应提供开放的二次开发接口，支持企业个性化业务场景的定制化开发。

5.3 基础设施要求

支撑平台互联互通的计算、存储、网络基础设施应满足高可用、高性能要求，计算资源应支持弹性伸缩，应对互联互通过程中的高并发请求；存储资源应采用分布式存储架构，保障跨云数据的安全存储与高效访问；网络基础设施应具备低延迟、高带宽的特性，支持跨云数据的高速传输，同时配置网络隔离、加密传输等安全措施。

6 核心互联互通技术要求

6.1 跨云资源纳管互联互通

应实现对主流云服务商的计算（ECS、CVM等）、存储（对象存储、块存储等）、网络（虚拟私有云、负载均衡等）、数据库、中间件等各类云资源的全类型纳管，纳管准确率应达到99%以上；支持资源的定时同步与实时更新，资源配置变更的同步延迟应不超过30秒；应实现跨云资源的统一标识与生命周期管理，支持资源的跨云创建、删除、修改、查询等标准化操作，操作指令的跨云执行成功率应达到99.9%以上。[源自：GB/T 35295，6.1]

6.2 跨云数据流动互联互通

应支持跨云数据的备份、迁移、实时同步等多种流动场景，兼容结构化、半结构化、非结构化等各类数据类型；应遵循算力互联互通数据流动相关标准，具备数据存储对接、全局数据共享、数据调度管理能力，支持跨地域、跨云平台的冷热温数据分层流动，数据流动的调度成功率应达到99.9%以上；应配置数据转换引擎，实现不同云平台数据格式的自动转换，保障数据流动的一致性；应支持数据流动的断点续传与容错处理，避免数据丢失或损坏。

6.3 跨云资源调度互联互通

应具备全局的资源状态感知能力，实时采集各云平台资源的负载、性能、成本等指标，构建统一的资源视图；支持基于预设策略（如负载均衡、成本最优、业务连续性）的跨云资源自动调度，如将高负载云平台的业务调度至低负载云平台，实现算力资源的跨云弹性伸缩；调度决策的响应时间应不超过10秒，调度操作的执行延迟应不超过1分钟；应支持人工干预的跨云资源调度，满足个性化的业务需求。

6.4 跨云业务部署互联互通

应支持容器化、虚拟化等多种业务部署形态的跨云协同，兼容K8s等主流容器编排平台，实现业务应用的跨云一键部署、升级、回滚；应具备业务跨云容灾能力，支持业务在不同云平台之间的快速故障迁移，迁移过程中业务中断时间应控制在业务允许范围内；应实现跨云业务部署的资源依赖自动解析，确保业务在跨云部署时的资源配套与环境一致性。

6.5 接口与协议互联互通

平台内部各模块、平台与云服务商、平台与企业业务系统之间的接口应采用通用、开放的协议与标准，优先采用RESTful API、gRPC等标准化接口协议；接口应具备良好的兼容性与可扩展性，支持版本管理与向下兼容；应提供标准化的接口文档，明确接口参数、返回值、调用方式等，保障接口调用的规范性与便捷性。[源自：GB/T 38636，6.5]

7 互联互通安全技术要求

7.1 网络安全

平台互联互通的网络传输应采用TLS/SSL等加密协议，确保数据与指令在传输过程中的机密性与完整性；应配置防火墙、入侵检测/防御系统，对跨云接入的网络流量进行监控与防护，防范网络攻击；应实现各云平台之间、平台与企业业务系统之间的网络隔离，根据业务需求配置细粒度的网络访问控制策略，禁止未授权的网络访问。

7.2 数据安全

跨云流动与存储的数据应进行分级分类管理，针对不同级别的数据采取相应的加密、访问控制措施；核心敏感数据应采用国密算法进行端到端加密，包括数据传输加密与存储加密；应建立跨云数据访问

审计机制，记录所有数据的访问、操作、流动行为，审计日志应保存不少于6个月；应禁止敏感数据的未授权跨云流动，满足数据合规与数据主权要求。

7.3 权限与身份安全

应建立统一的身份认证与授权体系，支持多因素认证、单点登录等功能，实现跨云资源与操作的统一身份管控；应基于最小权限原则，为不同角色分配细粒度的跨云操作权限，避免权限过度分配；应实现权限操作的全程审计，及时发现并处置越权操作、异常登录等行为；应支持权限的动态调整与回收，保障权限管理的时效性。[来源：GB/T 40657，7.3]

7.4 配置与运维安全

应建立跨云资源的标准化配置基线，实时监控资源配置状态，及时发现并处置配置漂移问题，配置漂移的检测发现时间应不超过1小时；应支持配置的一键回滚，确保资源配置的合规性与安全性；平台自身的运维操作应采用操作日志、运维审计等措施，防范运维过程中的人为安全风险；应定期对平台互联互通的安全策略、防护措施进行评估与优化。

8 互联互通性能与可靠性要求

8.1 性能要求

平台应支持至少10家以上云服务商的同时接入，单平台最大纳管云资源规模应不低于10000台计算实例；跨云接口的并发调用能力应不低于10000 TPS，接口调用的平均响应时间应不超过500ms；跨云数据流动的带宽应支持按需扩展，单任务最大数据传输速率应不低于100MB/s，小文件（小于1GB）跨云迁移的平均耗时不应超过5分钟；平台的可视化操作界面应具备良好的响应性，页面加载时间应不超过3秒。

8.2 可靠性要求

平台互联互通的核心服务模块应采用主备部署、集群部署等高可用架构，无单点故障，核心服务的可用率应达到99.95%以上；平台与云服务商的接入链路应配置多链路备份，单链路故障时应能实现秒级切换，确保接入的连续性；跨云操作与数据流动应具备容错处理能力，在网络波动、云平台临时故障等情况下，应能自动重试或暂停，故障恢复后继续执行，避免操作失败或数据丢失；平台应具备数据备份与恢复能力，核心的互联互通配置数据、审计日志应定期备份，备份数据的恢复成功率应达到100%。[源自：YD/T 3986，8.2]

8.3 可扩展性要求

平台应支持云服务商、云资源类型的无缝扩展，新增云服务商的接入适配周期应不超过7个工作日；平台的性能指标（如并发能力、纳管规模）应支持通过横向扩容实现线性提升；平台的功能模块应支持按需部署与升级，升级过程中应不影响平台互联互通的正常运行。

9 互联互通测试与验证

9.1 测试类型与内容

平台互联互通应开展功能测试、性能测试、安全测试、兼容性测试、可靠性测试等全维度测试。功能测试验证跨云资源纳管、数据流动、资源调度等核心互联互通功能的实现效果是否符合本规范要求；性能测试验证平台在高并发、大数据量场景下的响应时间、处理能力等性能指标；安全测试验证网络、数据、权限等安全防护措施的有效性；兼容性测试验证平台与不同云服务商、不同版本云平台、不同企业业务系统的兼容能力；可靠性测试验证平台在故障、异常场景下的可用性与容错能力。

9.2 测试方法与要求

测试可由平台研发方自行开展，也可委托具备相应资质的第三方测评机构实施；测试应制定标准化的测试方案，明确测试用例、测试环境、测试方法与判定标准；测试环境应模拟实际的多云部署场景，覆盖主流的云服务商与云资源类型；测试过程应做好详细记录，形成完整的测试报告，测试报告应包括测试内容、测试结果、问题分析、整改建议等。[源自：YD/T 4099，9.2]

9.3 验证与验收

平台互联互通建设完成后，应依据本规范及测试报告进行验收，验收合格后方可投入正式运行；验收应包括技术文档审查、现场功能演示、性能指标实测、安全漏洞扫描等环节；对于测试与验收过程中发现的问题，应限期整改，整改完成后重新进行测试与验收，直至符合要求。

10 运维与服务管理要求

10.1 日常运维管理

应建立常态化的平台互联互通运维管理机制，制定详细的运维操作手册，明确运维流程、岗位职责与操作规范；应实时监控平台互联互通的运行状态，包括接口调用状态、数据流动状态、资源调度状态、网络状态等，建立7×24小时的监控告警体系，告警响应时间应不超过15分钟；应定期对平台的软硬件设施、核心服务模块进行巡检，及时发现并处置潜在的故障隐患。

10.2 故障处置管理

应建立分级的故障处置体系，根据故障影响范围、严重程度将故障划分为不同等级，制定对应的故障处置预案；故障发生后，应按照预案快、排速开展故障定位查与处置，记录故障处置过程，形成故障处置报告；应建立故障复盘机制，对重大故障进行复盘分析，总结故障原因，优化防控措施，避免同类故障再次发生。

10.3 技术文档与记录管理

应建立完整的平台互联互通技术文档体系，包括架构设计文档、接口开发文档、部署实施文档、运维操作手册、测试报告等，技术文档应及时更新，确保与实际部署运行情况一致；应做好平台互联互通的运行记录，包括接口调用日志、数据流动日志、资源调度日志、告警日志、故障处置日志、运维操作日志等，所有记录应保存不少于2年，具备可追溯性。

10.4 技术服务与升级

平台运营方应向用户提供专业的互联互通技术服务，包括技术咨询、问题排查、操作指导等；应建立平台的持续升级与优化机制，根据云计算技术发展、行业标准更新、用户需求变化，及时对平台的互联互通功能、性能、安全进行升级优化；升级优化前应进行充分的测试验证，制定升级方案与回滚预案，确保升级过程的安全性、稳定性。