YDB

中 国 通 信 标 准 化 协 会 标 准

YDB XXX –201X

云计算运维平台参考框架及技术要求

Cloud computing operation and maintenance Platform reference framework and Technical specification

（征求意见稿）

201X –XX –XX 印发

中国通信标准化协会

目　　次

前　言

为培育国内公共云服务市场，增强用户对云服务的信心，保护正规云服务商，促进市场良性发展，指导企业更好地指导、帮助建设云计算运维平台，云计算发展与政策论坛开展可信云服务认证云计算运维管理平台建设分级分类评估标准的编写工作。

本标准旨在指导云计算企业建设云计算运维平台体系，并从云计算运维平台的IaaS管控层、原子平台层、PaaS层以及运维场景层四个部分描述了云计算运维解决方案的分级分类评估标准及具体的评估方法。

本标准按照 GB/T 1.1-2009 给出的规则起草。

本技术报告由中国通信标准化协会提出并归口。

本技术报告起草单位：

本技术报告主要起草人：

云计算运维平台参考框架及技术要求

1 范围

本标准规定了云计算运维平台参考框架及分层技术要求，分别为IaaS管控层、原子平台层、PaaS层和运维场景层，以及各层需具备的分级技术要求。

本标准适用于公有云、私有云、混合云等多种场景下的云计算运维平台的建设，旨在为企业建设云计算运维平台提供指导，也可供重点行业和其他企事业单位参考。云计算运维平台建设可不限于本标准的指标项或条款项；或可以根据不同业务不同用户需求，适当裁剪本标准中的指标项或条款项，但涉及到本标准中的指标项或条款项，应符合标准中的定义和规范性描述。

2 规范性引用文件

下列文件中的条款通过本部分的引用而成为本部分的条款。凡是注日期的引用文件，仅所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。

[1] GB/T 32400-2015 信息技术 云计算 概览与词汇
[2] GB/T 32399-2015 信息技术 云计算 参考架构
[3] YD/T 1926.1-2009 IT运维服务管理技术要求 第1部分 体系架构
[4] YD/T 1926.2-2009 IT运维服务管理技术要求 第2部分 管理服务定义
[5] YD/T 1926.3-2009 IT运维服务管理技术要求 第3部分：服务管理流程
[6] YD/T 2008-H85 IT运维服务管理技术要求 第4部分 服务管理支撑系统
[7] YD/T 1926.5-2010 IT运维服务管理技术要求 第5部分：配置管理数据库

3 术语和定义

下列术语和定义适用于本文件。

3.1 信息技术基础架构库 Information Technology Infrastructure Library

为IT服务管理提供集成及基于流程的最佳实践库，提供管理方法来达成使用信息系统的业务有效性和高效性。

3.2 公有云 Public cloud

云服务可以被任意云服务客户使用，且资源被云服务提供者控制的一种云部署模型。

3.3 私有云 Private cloud

云服务仅被一个云服务客户使用，且资源被该云服务客户控制的一类云部署模型。

3.4 混合云 Hybrid cloud

至少包含两种不同的云部署模型的云部署模型。

3.5 基础设施即服务 Infrastructure as a Service

提供给消费者的服务是对所有计算基础设施的利用，包括处理CPU、内存、存储、网络和其它基本的计算资源，用户能够部署和运行任意软件，包括操作系统和应用程序。消费者不管理或控制任何云计算基础设施，但能控制操作系统的选择、存储空间、部署的应用，也有可能获得有限制的网络组件（例如路由器、，防火墙，、负载均衡器等）的控制。

3.6 平台即服务 Platform as a Service

提供给消费者的服务是把客户采用提供的开发语言和工具（例如Java，Python, .Net等）开发的或收购的应用程序部署到供应商的云计算基础设施上去。客户不需要管理或控制底层的云基础设施，包括网络、服务器、操作系统、存储等，但客户能控制部署的应用程序，也可能控制运行应用程序的托管环境配置。

3.7 软件即服务 Software as a Service

提供给客户的服务是运营商运行在云计算基础设施上的应用程序，用户可以在各种设备上通过客户端界面访问，如浏览器。消费者不需要管理或控制任何云计算基础设施，包括网络、服务器、操作系统、存储等。

3.8 企业服务总线 Enterprise Service Bus

它是传统中间件技术与XML、Web服务等技术结合的产物。ESB提供了网络中最基本的连接中枢，是构筑企业神经系统的必要元素。ESB的出现改变了传统的软件架构，消除不同应用之间的技术差异，让不同的应用服务器协调运作，实现了不同服务之间的通信与整合，提供比传统中间件产品更为廉价的解决方案。

3.9 DevOps

英文Development和Operations的组合，是一组过程、方法与系统的统称，用于促进开发（应用程序/软件工程）、技术运营和质量保障（QA）部门之间的沟通、协作与整合。它的出现是由于软件行业日益清晰地认识到：为了按时交付软件产品和服务，开发和运营工作必须紧密合作。

3.10 BT（BitTorrent）

一种内容分发协议，采用高效的软件分发系统和点对点技术共享大体积文件，并使每个用户像网络重新分配结点那样提供上传服务，分配器或文件的持有者将文件发送给其中一名用户，再由这名用户转发给其它用户，用户之间相互转发自己所拥有的文件部分，直到每个用户的下载都全部完成。

3.11 Overlay

是一种网络架构上叠加的虚拟化技术模式，在对基础网络不进行大规模修改的条件下，实现应用在网络上的承载，并能与其它网络业务分离，并且以基于IP的基础网络技术为主。Overlay 技术是在现有的物理网络之上构建一个虚拟网络，上层应用只与虚拟网络相关。一个Overlay网络主要由三部分组成：边缘设备（是指与虚拟机直接相连的设备），控制平面（主要负责虚拟隧道的建立维护以及主机可达性信息的通告），转发平面（承载 Overlay 报文的物理网络）。

4 缩略语

下列缩略语适用于本文件。

API	Application Programming Interface	应用程序接口
APaaS	Application Platform as a Service	应用平台即服务
BT	BitTorrent	文件分发协议
C/S	Clinet/Server	（客户机/服务器）
CI/CD	Continuous Integration/ Continuous Delivery	持续集成/持续交付
CMDB	Configuration Management Database	配置管理数据库
CPU	Central Processing Unit	中央处理器
DB	Database	数据库
ESB	Enterprise Service Bus	企业服务总线
TSDB	Two-step direct bonding	双阶梯（硅片）直接键合
KV	key value	键值
IDC	Internet Data Center	互联网数据中心
IPaaS	Integration Platform as a Service	集成平台即服务
SDK	Software Development Kit	软件开发工具包
SOA	Service-Oriented Architecture	面向服务的架构

5 云计算运维平台体系参考框架及分层技术要求

云计算运维平台用于企业对IT资源的运维管理，依托SOA设计理念将云计算运维平台以IaaS管控层、原子平台层、PaaS层、运维场景层输出服务，提供各层资源全生命周期的运维管理，实现对企业IT资源的集中化、可视化、自动化管理。

IaaS管控层：是指对IaaS的管理和控制，通过提供指令、文件、数据下发的管道，适配各类型主机（Linux、Windows、小型机、虚拟机、容器等），兼容私有云、公有云以及混合云的管理方式；

原子层：是指为满足通用运维场景的基础能力平台的封装，由作业功能模块、CMDB模块、运维数据平台模块、容器管理模块、智能运维模块等功能模块组成。

PaaS层：包含支持应用部署和运行的APaaS（Application Platform as a Service)以及企业内部SOA集成的IPaaS（Integration Platform as a Service），通过企业服务总线和API Gate Way对接原子层各平台的能力。

运维场景层：是指基于PaaS层之上构建的运维SaaS，涵盖基础运维、监控告警、ITIL流程、DevOps、任务编排、弹性伸缩、安全审计等各领域。

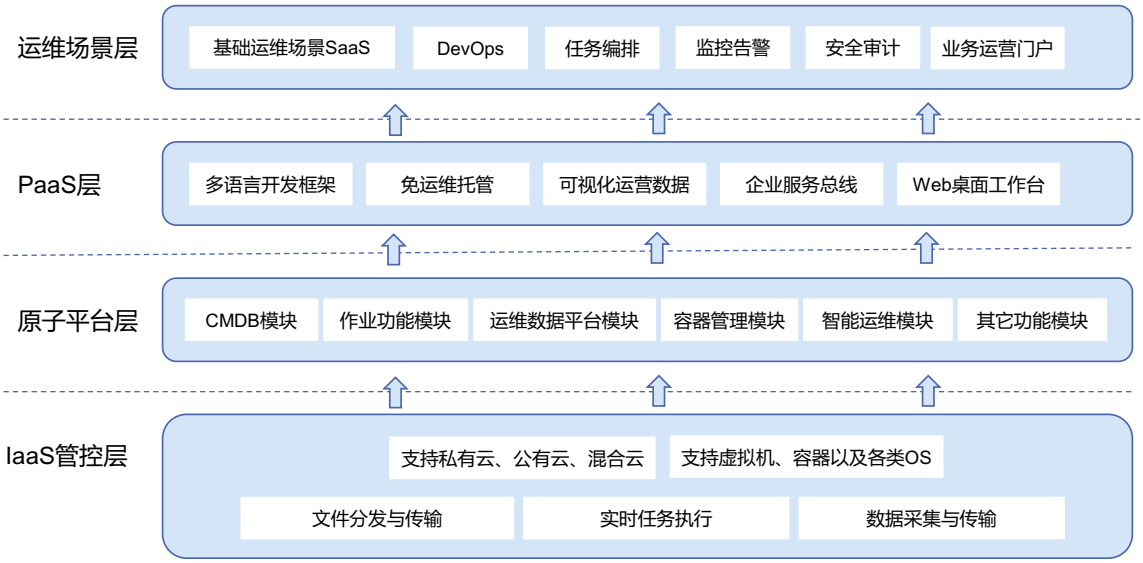

图 1 云计算运维参考框架

5.1 云计算运维管理平台各功能模块关系

本节通过2个运维场景来阐述云计算运维管理平台各功能模块关系。

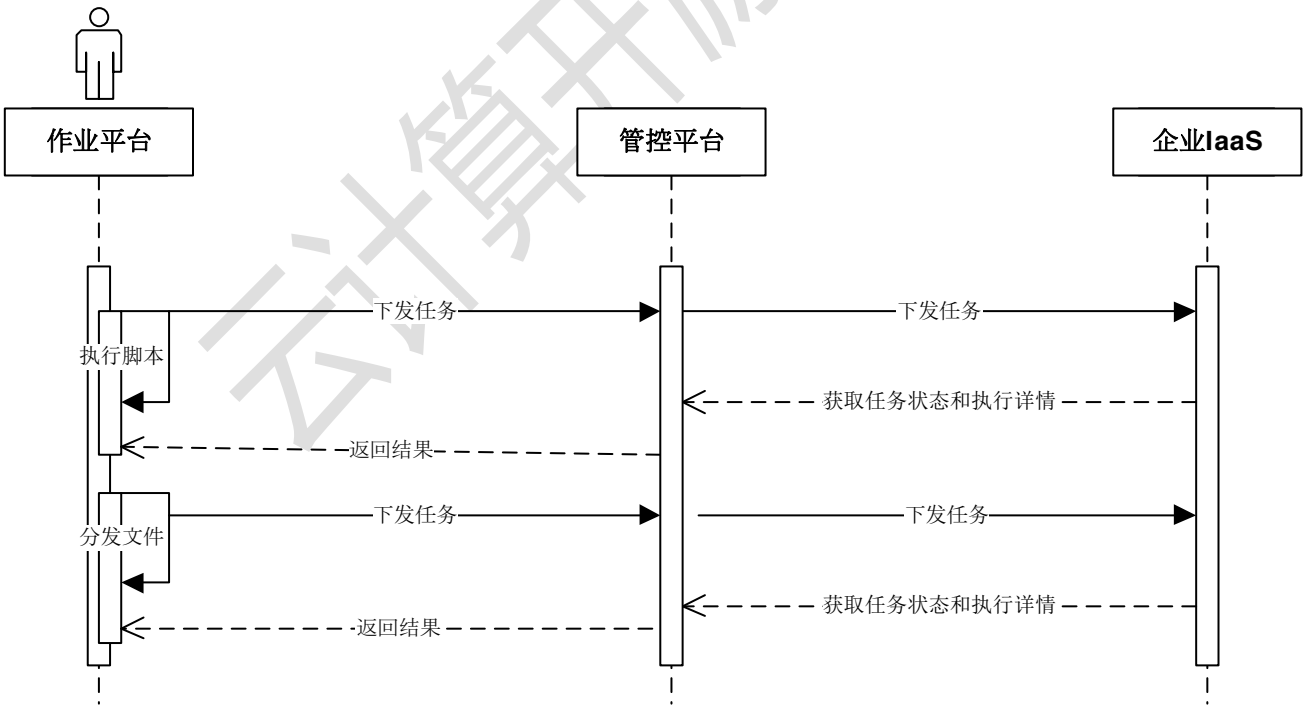

图 2 运维脚本执行、分发文件运维场景事件流

上述是运维场景中常见的脚本执行、文件分发的时序图：作业平台下发脚本执行或文件分发的任务至管控平台，管控平台在企业IaaS层完成对应任务后获取任务状态和执行详情，作业平台获取上述任务状态和执行详情呈现给用户。

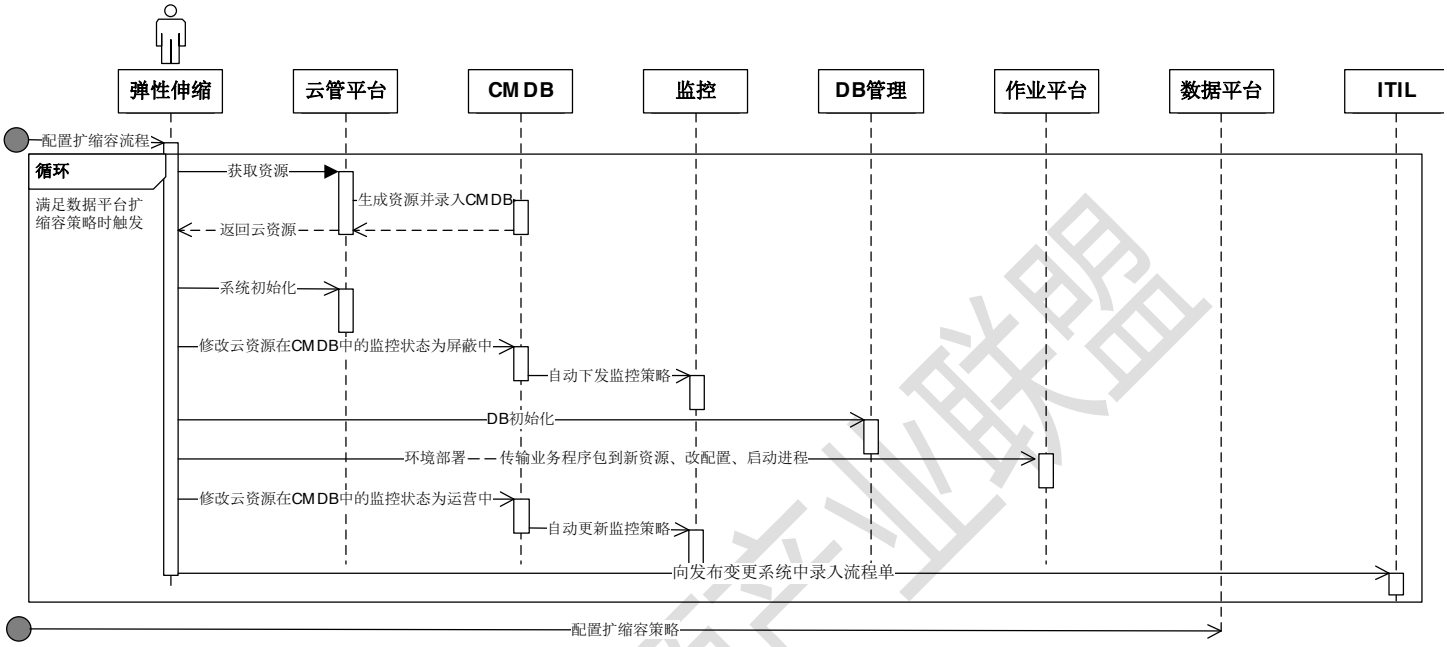

图 3 业务扩缩容场景事件流

以上是业务扩缩容场景的时序图：首先在弹性伸缩产品上配置完扩缩容流程，扩缩容策略会下发至数据平台。当满足扩容策略时触发扩容动作，向云管平台获取资源并录入CMDB，然后进行系统初始化，把云资源在CMDB中的监控状态调整为屏蔽中，对应监控策略下发至监控系统。接下来在DB管理系统中完成DB初始化，通过作业平台完成环境部署（传输业务程序包到上述获取的云资源并修改配置、启动进程），然后修改云资源在CMDB中的监控状态为运营中，自动更新监控策略，最后在发布变更系统录入流程单完成本次扩缩容事件。

5.2 IaaS 管控层

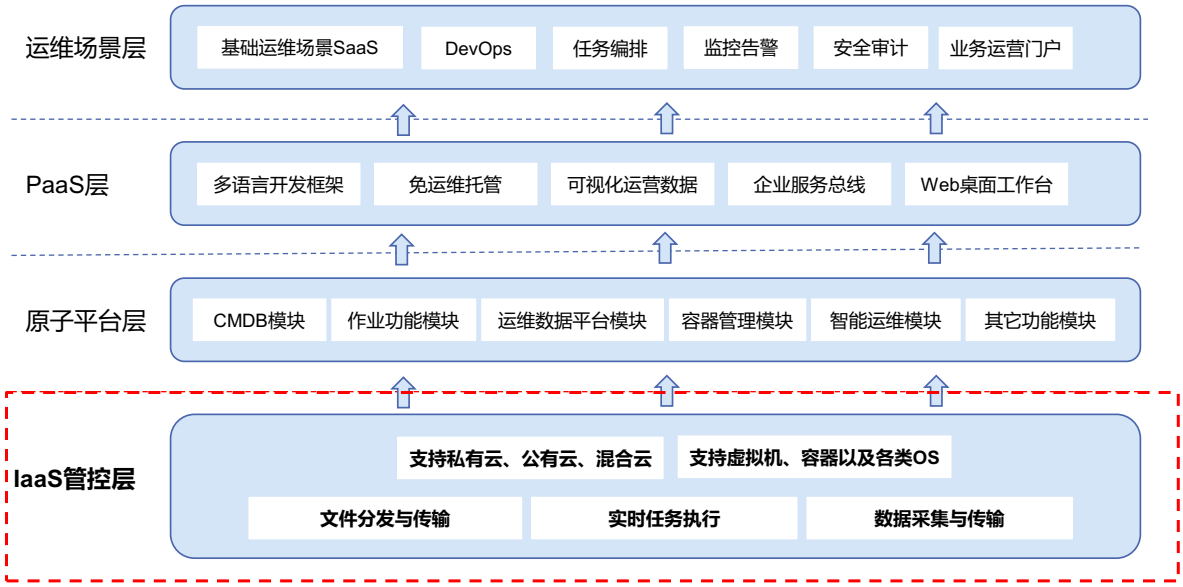

图 4 IaaS 管控层

5.2.1 IaaS 管控层定义

IaaS管控层是整个云计算运维框架的底层支撑体系，是上层运维场景与底层IaaS的连接器，为上层提供指令、文件、数据的通道，支持直连、代理以及为达到最优连接指定级联路由方式的模式。管控层需采用分布式C/S结构，主要包含智能Agent、提供各种功能服务的Server以及Zookeeper、Redis、MySQL等模块。

示例1：Agent 为部署在业务机器上的程序，每台业务机器理论上只可以部署一个 Agent，其他模块部署无具体要求，支持单独部署、混合部署两种模式。

在云计算运维体系建设中，管控层为各平台模块提供了人机交互的通道与能力，并提供三种类型的服务能力：文件分发传输能力、命令实时执行与反馈的能力、大数据采集与传输的能力。

5.2.1.1 支持私有云、公有云、混合云

IaaS 管控层能够适配企业内 IDC、各类公有云的独立管控以及混合云的统一管控：

a) 对于企业内 IDC，支持 Agent 直连模式管控；

b) 对于公有云管控，可通过设置 Agent 为代理模式，实现对该片区域云主机的管控；

c) 对于网络隔离区域的管控，具备设置指定级联路由的方式实现对其管控。

5.2.1.2 支持虚拟机、容器以及各类 OS

能够支持适配主流Linux、Windows、AIX版本以及对低层虚拟技术和容器的兼容。

5.2.1.3 文件分发与传输

文件分发是指用户从指定机器将指定文件批量传输到特定范围的机器上。文件分发是用户行为，传输则是针对用户行为的程序行为。

文件分发传输的主要功能点：

①传输模式：

——支持BT模式:是指对于10KB上的文件分发自动启用BT作为首选传输方式,提升文件的分发效率以及避免拥塞；

——支持直传模式：是指针对10KB下（含10KB）的文件使用TCP直传模式；

——支持混合模式：是指在BT模式传输持续性失败，则会尝试使用直传模式传输BT文件分片；当BT传输恢复时，则停止直传模式；

②传输类型：

——文件传输：是指将多种格式、可读目录下的单个文件分发到指定机器；文件分发完成后，自动同步目标文件权限与源文件一致；对于直传模式，文件传输结束后进行MD5校验，对于BT模式和混合模式，则进行哈希值校验文件的完整性；

——目录传输：用户将指定目录分发到多台机器指定可写目录下。目录分发将保持源目录结构和权限不变；

——正则匹配传输：用户通过通配符（符合通用正则规则）指定多个文件，并传输到指定机器的指定可写目录。传输完成后文件的格式和权限与源文件保持一致。

例如：将A服务器/data/目录下的所有以 .log 结尾的日志文件传输至B服务器的/data/log/目录下。

③传输控制：

——区域链控制：是指通过设定规则，使文件只能在两个区域间单向传输，以满足具有特殊专线链接的两个区域间的传输需求。

注：特定安全场景：文件只能从A私有云区域传输至B私有云区域，反之则无法传输。

——跨区域穿透：是指原本相互隔离的两个区域需要进行文件传输，需对本次传输进行定向穿透。管控平台允许权限用户适当修改配置来完成这种定向穿透。

5.2.1.4 实时任务执行

①任务类型：

——命令类型：Linux 支持 bash 命令、Windows 支持 cmd 命令、AIX 支持 ksh 命令，支持自定义可执行文件格式程序的启动，支持解释性语言程序的执行。

——脚本类型：Linux 支持 Shell 脚本、Windows 支持 bat 脚本（安装有 Cygwin 的额外支持 Shell 脚本）、AIX 支持 ksh 脚本，以及各种系统支持的解释性脚本程序。

②任务控制：

——指定用户：是指 Linux 及其他类 Linux 系统支持按指定用户执行任务。

例如：用户设定以 Mysql 用户执行 cat /etc/shadow 命令查看 shadow 文件内容（返回 Permission denied），可以知道 Mysql 无法查看该文件，Mysql 只能查看该用户权限范围内的结果；由于 Windows 操作系统的限制，需开启校验机器密码功能的用户才能指定用户执行任务，否则都以 Administrator 用户执行任务。

——继承用户环境：是指 Linux 及其他类 Linux 系统支持指定用户后继承该用户设定的环境变量；Windows 可无此功能。

——校验机器密码：是指用户选择校验机器密码，Windows Agent 按指定用户执行任务的功能。

——有害操作告警：是指管控系统能够自动设定高危操作的定义，并支持对高危操作进行预警。

——有害操作防护：管控系统能够自动识别高危操作，对高危操作进行预警和干预，高危操作的定义及干预措施提供选项供用户配置。

5.2.1.5 数据采集与传输

①数据采集服务：

——自定义数据采集：Agent 开放数据发送接口、cmdline 及 SDK，提供用户开发自定义的数据采集程序或脚本。

——采集器插件化支持：Agent 支持采集器插件化，自动加载采集插件，并监控插件的存活状况。如果采集插件异常终止，则重新拉起采集插件；如果连续拉起失败超过 4 次则触发告警。

——实时数据快照：管控层支持缓存安装有 Agent 的机器 1 分钟内的快照数据，并提供接口供用户访问。

——动态负载均衡：由于 Agent 数据采集的量大，且具有随业务特性波动的特点，数据在流转时需要高性能的服务端做收敛转发，为提供服务端机器的利用率，减少由于数据量变化时带来的负载不均衡问题，管控系统支持按分钟

级别动态调整数据转发的通道，以达到集群内服务端负载均衡的目的。

②集群管理

——自动服务发现：管控平台同一个集群内的模块均支持自动发现，用户可以扩容、缩容任何节点，系统均能实时感知，并调整通讯策略，保证服务的高可用。

——集群负载均衡：管控平台同一个集群内，支持按照 Agent 链接数进行负载均衡。

——Agent 状态查询：管控平台提供接口，查询 Agent 状态。接口按照实时性分为两类：一类为实时状态接口，支持查询当前 Agent 是否正常；二类接口提供 24s 内的状态查询，查询的内容包括 Agent 上次心跳时间、Agent 版本、Agent 使用的 CPU、Agent 使用的 Memory。

——多区域负载均衡：管控平台支持对同一集群进行不同区域的划分，不同区域按照各区域内的负载均衡规则处理；未划分区域的 Agent 按照集群负载均衡策略处理。

5.3 原子平台层

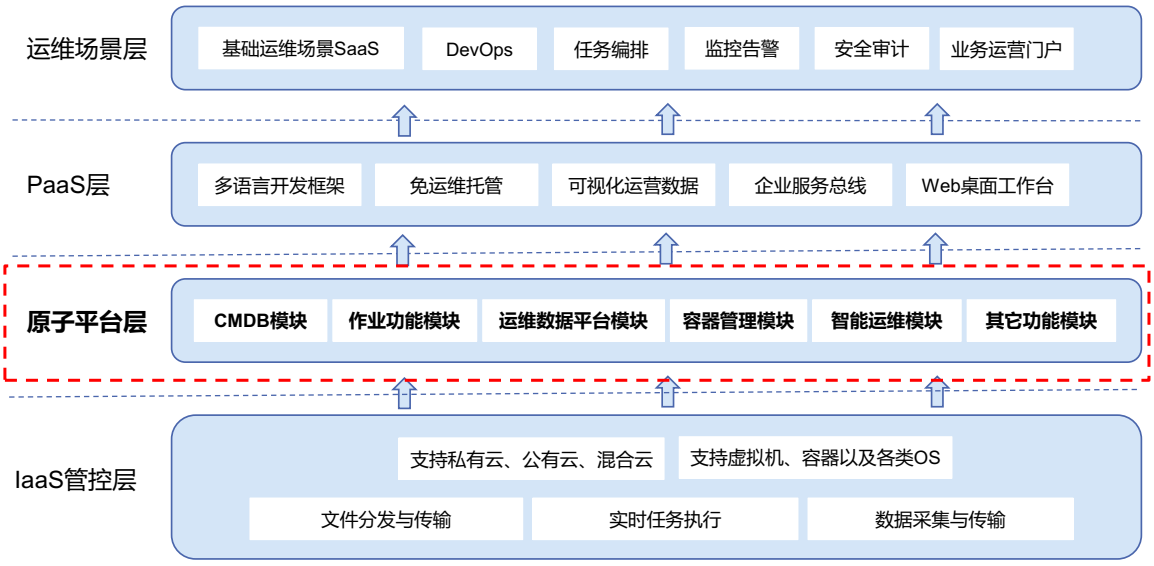

图 5 原子平台层

5.3.1 原子平台层定义

本指标项定义为IaaS层之上的管理与基础运维操作平台，具体包括：运维操作对象管理的CMDB模块，运维执行脚本和文件传输的作业功能模块，对基础设施、应用程序、中间件等各类环境的运行状态进行数据采集和分析的运维数据平台模块，对容器的镜像生产、管理、资源调度的容器管理模块，以及建设智能化运维为目标的功能模块，等其它满足运维基础操作的独立统一功能模块。

5.3.2 CMDB 模块

配置管理数据库（CMDB）是构建其它流程的基础，CMDB作为面向业务层面的CMDB，为云计算运维体系的其它平台提供了各种运维场景的配置数据服务，存储与管理企业IT架构中设备的各种配置信息，它与所有服务支持和服务交付流程都紧密相联，并依赖于相关流程以保证数据的准确性。

5.3.2.1 业务层面的主机资源管理

主机资源基于业务层面进行管理，拓扑维度的资源概况展示，并能支持外部资源的导入和云主机的实时同步，同时支持跨云管理主机；对于不同类型业务的主机资源，具备自定义属性的扩展功能。

5.3.2.2 业务拓扑资源管理

业务拓扑是CMDB进行主机管理的基础，合适的业务模型决定主机的结构化管理，CMDB需提供用户结构自定义、拓扑属性自定义等功能，可以针对不同的场景选择性的建立适合于业务的结构。

5.3.2.3 业务管理

支持面向不同角色提供业务的权限级别管理和业务的增删改查等操作，并且所有运维操作平台的权限都以CMDB为核心。

5.3.2.4 自定义属性管理

CMDB提供自定义模型属性适配所有各类业务场景,用户可以基于业务、集群、模块和主机上新增自定义属性, 同时可在CMDB中自定义主机属性时关联主机自定义采集策略，实时下发采集策略到线上主机并上报数据到CMDB，供周边系统使用。

5.3.2.5 进程端口与配置文件管理

可以将业务的进程、端口、配置文件注册到CMDB，并关联到业务拓扑中，为上层的应用比如监控、进程管理等提供数据和配置服务。

5.3.2.6 对象管理

可根据用户需求自定义管理的对象类型，新增的对象类型可以关联到具体的业务拓扑，也可以提供对应的增删改查API供周边系统使用。

5.3.2.7 资源分组

CMDB中提供静态数据与动态数据两种配置数据，资源分组功能可以结合动静态数据对资源进行任意组合，供周边系统使用。

5.3.2.8 数据审计

将动态数据与CMDB中的已存在静态数据进行周期性对比，当数据不一致时，进行告警并给出统一对比结果。

5.3.2.9 操作审计

是指所有用户在CMDB上的操作都有对应的记录可供追溯，并且所有操作审计记录都需录入到事件中心。

5.3.3 作业功能模块

作业功能模块是底层基于管控之上的基础运维操作平台，具备海量的并发处理能力，支持脚本执行、文件拉取/分发、定时执行等多种可实现的基础运维场景，还支持单个任务组装成一个作业流程。同时，可通过平台提供的API实现对任意作业的调用、查看等操作，与其它平台或系统联动，实现调度自动化。

5.3.3.1 传输文件方式

管控平台的Agent可触发作业平台的任务执行和文件传输，使用BT（BitTorrent）方案应对大文件传输，使得文件拉取和传输更高效。文件的拉取和传送更加便捷，可支持的“多对多、多对一”的多模式文件分发传输任务。

5.3.3.2 Web 化脚本管理

云化脚本管理模式，支持多个协作者通过平台进行脚本共享使用，同时支持脚本单独执行，也支持多个脚本或文件传输流程串接组合成作业任务。

5.3.3.3 支持批量高效执行

针对运维场景中的多服务器操作须能够支持企业服务器管理规模扩大之后的并发执行任务能力。

5.3.3.4 作业编排

支持作业平台的文件传输、脚本执行等原子步骤编排为作业流程，实现复杂场景下的自动化作业执行，以便后续的管理和复用。

例如：在版本发布运维场景下，往往需要执行多个步骤：分发新的版本文件到各节点服务器、停止进程、更新版本、启动进程，每一步所操作的对象都不同，可以通过作业平台将以上的各步骤按照如上顺序编排成作业。

5.3.4 运维数据平台模块

运维数据平台模块是指运维领域的低门槛大数据平台，支持数据接入、清洗、计算、存储、查询和分析的全流程自助化大数据服务，运维人员可以通过统一数据接入、可视化计算任务配置、可视化建模、统一查询等功能，快速的构建基于大数据的可视化、智能化运维支撑工具。

5.3.4.1 统一数据接入

统一数据接入提供了数据采集、数据汇聚、数据清洗、数据传输的全自助化的服务，目标是最大化降低数据接入门槛、提升数据接入的效率和质量。用户无需登录服务器进行操作和故障排查，就可接入数据，数据类型包括：基础性能、组件日志、业务日志、DB数据、自定义上报、HTTP等。

5.3.4.2 可视化计算配置管理（DataFlow）

DataFlow是将业务运维数据的实时计算、离线计算、算法分析等一系列复杂数据处理相融合的一种计算方式，用户使用标准的SQL和拖拽功能就可以构建一个复杂的，多层级的混合计算逻辑。运维数据平台DataFlow是可以同时配置管理实时计算与离线计算，一份原始数据的整个处理流程可以在DataFlow中体现，用户可以基于DataFlow进行实时、离线数据计算，数据过滤等复杂数据处理。

5.3.4.3 可视化建模管理（ModelFlow）

ModelFlow是将业务运维的数据分析挖掘低成本化，将机器学习算法原子节点化，将模型的构建过程标准化。用户可以按照标准流程通过拖拽配置原子节点，完成数据分析挖掘模型的构建，解决运维中的数据挖掘问题。ModelFlow与 DataFlow深度集成，ModelFlow运行实例可以与实时计算、离线计算组合成DataFlow，完成了从构建到实例运行的整个闭环。

5.3.4.4 运维数据存储查询

通常存储类型分为：关系型、KV型、时序型、全文检索型和分析型，根据运维数据的类型（基础运维数据、时间序列数据、文本事件数据）、大小和使用场景，将运维数据分类存储，基础运维数据（运维元数据）使用关系型存储和KV型存储适用于运维信息明细查询，文本事件数据使用全文检索引擎，时间序列数据使用场景比较广泛，用于实时监控存储需要使用TSDB存储，用于多维度数据分析，需要分析型存储支持，以及历史数据的保存和归档需要离线存储。

数据类型	应用场景	查询实时性	存储类型	存储选型
基础运维数据	运维元数据	高	关系型存储	MySQL，SQLite

	状态数据 KeyValue	高	KV 型存储	Redis，Hbase
时间序列数据	监控告警	高	TSDB 型存储	InfluxDB，OpenTSDB
	数据分析、视图展示	高	分析型存储	Druid、CrateDB
	历史数据归档	准实时	文件系统	HDFS，S3
文本事件数据	全文检索	高	检索型存储	Elasticsearch、Solr

表 1 运维数据存储查询

5.3.5 容器管理模块

容器管理平台是以容器技术为基础，支持为开发者和企业提供应用的镜像构建、镜像仓库、容器编排和调度、容器部署和运维管理的云计算平台，其中包括标准化、容器存储服务、容器鉴权、大规模、可伸缩的容器托管服务以及集群混合管理服务。实现微服务架构集群系统，帮助客户实现应用业务在容器云平台上的快速部署。

5.3.5.1 应用仓库

是指镜像包含用户所需的操作系统、运行时环境和应用程序，支持部署集群或创建容器实例。镜像仓库分为公开仓库和私有仓库，主要用于存放镜像。应用仓库对高可用以及安全有很高的要求，以保障镜像得到及时获取和分发。

5.3.5.2 容器编排和调度服务

容器云平台提供容器编排和调度服务，支持应用集群一键部署，云计算资源弹性扩展，容器编排和自定义调度等功能，为用户提供了高性能的容器集群管理方案。支持弹性伸缩、垂直扩容、灰度升级、服务发现、服务编排、错误恢复、性能监测等功能，让应用能够快速部署服务。

5.3.5.3 多环境一致性管理

是指保证开发、测试、生产环境的一致性，能够有效的提高系统运行的稳定性。在容器技术能够支撑有效的解决方案提高多环境的一致性问题；容器技术实现了操作系统和硬件间的解耦，便于运维技术人员能及时发现不同系统间的差异，并根据这些差异进行调配，避免出现系统运行错误等情况。

5.3.5.4 容器网络服务

是指平台需提供SDN网络向虚拟机和容器提供统一的overlay网络，以及服务导出和负载均衡的功能。

5.3.5.5 容器安全服务

是指容器管理平台支持冗余、自恢复、高可扩展模型并具备基础安全能力；需结合安全基础防护、安全监测管理、安全运维等，形成完整的容器管理平台安全防护体系。

5.3.5.6 监控一体化和日志查询服务

监控平台一体化能够支持容器以及容器间通信进行自定义监控和展示，采用事前预警和事后报警的机制，保证应用可靠性，帮助运维人员快速发现、定位问题，并将应用从失效状态进行恢复，为应用的健康运行提供多方位的可靠性保证。另外，提供容器日志的统一查询服务，帮助运维可以根据不同日志维度定位应用程序问题以及日志查询。

5.3.6 智能运维模块

智能运维模块是指在运维领域能够提供数据分析挖掘服务，主要目标是降低运维领域数据分析挖掘的门槛。能够提供拖拽式建模、交互式测试调优、自动化模型评估、模型训练运行管理、场景模型(公共的通用的模型)等功能，包含了从模型构建评估到模型发布管理整个的功能链路，通过将各种基础的数据挖掘、机器学习算法节点化，将模型构建的过程标准化，使数据分析挖掘工作简单化。

5.4 PaaS 层

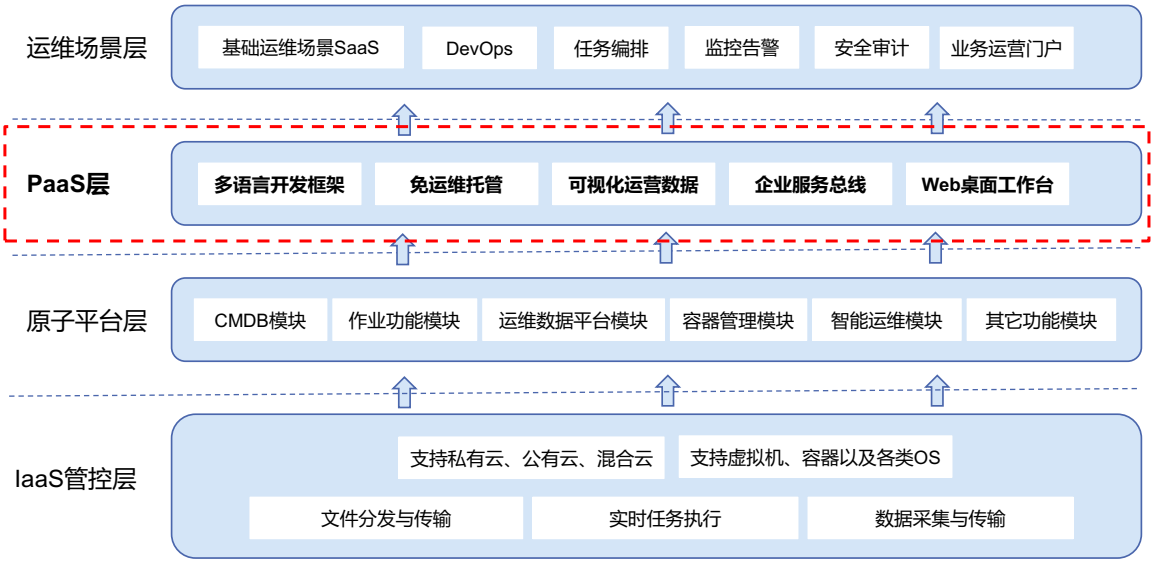

图 6 PaaS 层

5.4.1 PaaS 层定义

本指标项定义为PaaS层是一个开放的平台层，包含用于支持用户简单快速的创建、部署和托管应用的APaaS（Application Platform as a Service），以及提供了完善的前后台开发框架、服务总线（ESB）、调度引擎、公共组件等模块的IPaaS（Integration Platform as a Service）。PaaS层为一个应用从创建到部署，再到后续的维护管理提供了完善的自助化和自动化服务，如日志查询、监控告警等。

5.4.1.1 支持多语言的开发框架

PaaS提供支持多语言的开发框架，平台之上支持Python、php等技术语言开发运维自动化工具。开发框架集成统一登录鉴权模块、功能开关模块、WEB安全防护模块、功能组件模块等通用模块。

示例2：功能开关模块，如，支持开发者在 SaaS 开发迭代中对功能选择性开放、灰度测试等。

示例3：WEB 安全防护模块，如，防 csrf 攻击和防 xss 攻击。

5.4.1.2 免运维托管

PaaS提供从SaaS的创建、部署以及维护管理均实现免运维托管服务。运维人员开发的SaaS在平台采用分布式部署方式，一键自动部署。同时，SaaS部署使用Docker进行隔离，提高SaaS安全性。开发者可以主动通过PaaS的日志查看功能来查看日志记录和日志监控告警服务，开发者可以自定义配置相应的告警参数、告警接收人等信息，实时监控日志数据。

示例4：如，某一台承载服务器宕机之后，用户请求会被转发到备用服务器之上，保证 SaaS 工具的高可用

5.4.1.3 SaaS 运营数据可视化

PaaS提供SaaS的运营数据，运维人员需增强对运营数据的使用价值，包括其用户访问量、在线时长，活跃度等指标，综合展示该SaaS的使用情况。针对应用的Docker容器所占用内存和CPU进行实时监控统计，供用户了解应用的CPU和内存使用情况。

5.4.1.4 企业服务总线&API GateWay

作业功能模块、CMDB、数据平台、容器管理模块等原子平台统一开放API以组件的形式对接企业服务总线&API GateWay，实现各原子平台API协议统一和集中化管理，在上层的应用场景对API统一通过企业服务总线&API GateWay进行调用。同时，在企业服务总线&API GateWay上实现了对组件的权限校验、频率控制、访问统计、路由分发以及自助接入等功能。

5.5 运维场景层

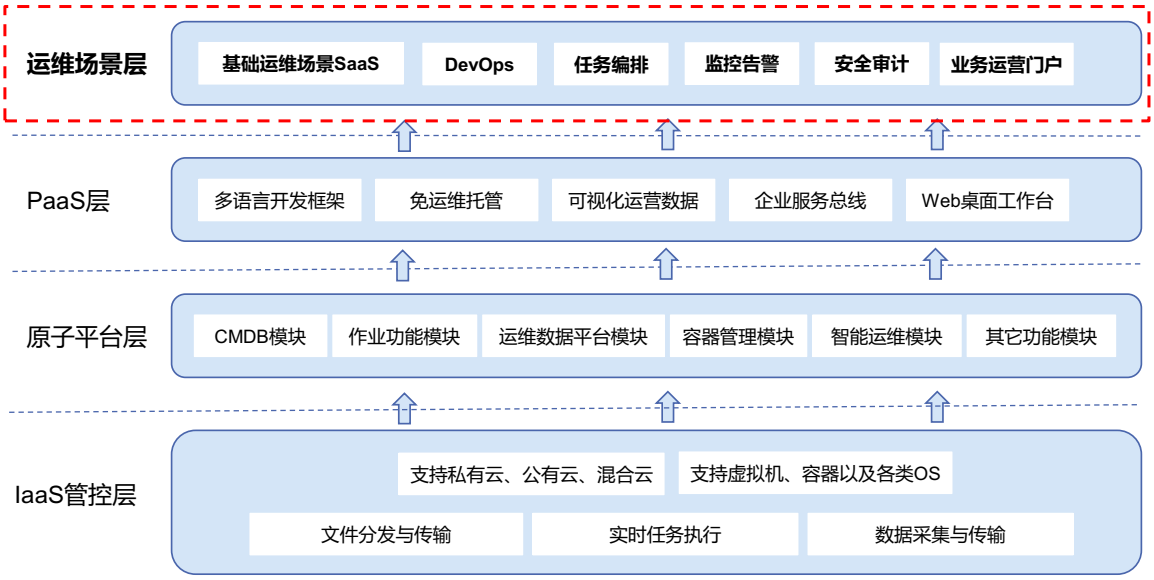

图 7 运维场景层

5.5.1 运维场景层定义

本指标项定义为应用场景SaaS是基于PaaS之上快速构建的面向运维场景解决方案的载体。它通过对底层各平台能力原子功能的拼装，实现基础运维、CI/CD、监控告警、任务编排、弹性伸缩、安全审计、ITIL以及移动运维等各类场景的自动化。

5.5.1.1 基础运维

针对运维工作中的日志查看、数值调整、数据提取、性能展示、配置变更等基础运维的自动化。

5.5.1.2 CI/CD

针对代码集成、构建、检查、测试 、布署、缺陷管理以及版本管理，实现全链路的自动化和可视化。

5.5.1.3 监控告警

实现主机性能、日志、自定义属性、应用性能、公共组件以及调用链等指标的监控告警，并能针对有确定处理流程的告警实现故障自愈。

5.5.1.4 任务编排

基于原子组件的封装和编排，并支持原子的自助开发接入，实现各异构平台间的无缝连接，解决运维场景操作全流程的调度自动化。

5.5.1.5 弹性伸缩

根据容量、负载评估以及在线预测等智能决策模型，实现无人值守的弹性伸缩。

5.5.1.6 安全审计

针对运维日常操作的高危扫描、行为监控、审计对帐，实现运维操作记录和操作结果的可追溯性。

5.5.1.7 移动运维

将部分简易固化的临时操作以及信息通知在移动端呈现，并可通过即时通讯工具的上下行实现部分交互的执行。

6 评判标准

从功能、效率、可靠性、可移植性以及可维护性等方面，评估得出云计算运维平台建设的完备性（Completeness 1 - Completeness 3,以下简称C1-C3），其中C1为最低等级，C3为最高等级。

从功能、能力方面，评估得出云计算运维平台建设的解决方案能力分级（Solution 1 - Solution 3,以下简称S1-S3），其中S1为最低等级，S3为最高等级。

附 录 A
（规范性附录）
云计算运维平台建设完备性分级

分层	项目	技术要求			备注
		C1	C2	C3	
功能					
IaaS 管控层	跨云管理	私有云	私有云、公有云	私有云、公有云、混合云	--
	适配主机类型	X86 服务器	X86 服务器、虚拟机、容器	X86 服务器、虚拟机、容器、小型机	
	适配操作系统	Linux、Windows		Linux、Windows、AIX 等其他类 Unix 操作系统	
	文件传输模式	直传模式	BT 模式、直传模式	BT 模式、直传模式、混合模式	--
	文件传输类型	文件传输	文件传输、目录传输	文件传输、目录传输和正则匹配传输	
	文件传输控制	不适用	区域链控制	区域链控制、跨区域穿透	
	执行任务类型	Windows 下的 BAT 或 PowerShell、Linux 下的 Shell	Windows 下的 BAT 或 PowerShell、Linux 下的 Shell,AIX 下的 ksh		--
	执行任务控制	指定用户、继承用户环境、校验机器密码	指定用户、继承用户环境、校验机器密码、有害操作告警、有害操作防护		--
	数据采集服务	自定义数据采集	自定义数据采集、采集器插件化支持	自定义数据采集、采集器插件化支持、实时数据快照、动态负载均衡	--
	数据采集集群管理	自动服务发现、Agent 状态查询	自动服务发现、Agent 状态查询、集群负载均衡	自动服务发现、Agent 状态查询、集群负载均衡、多区域负载均衡	--
原子平台层	CMDB	基于业务层面的主机资源管理、业务拓扑资源管理、业务管理	基于业务层面的主机资源管理、业务拓扑资源管理、业务管理、自定义属性管理、进程端口与配置文件管理、操作审计	基于业务层面的主机资源管理、业务拓扑资源管理、业务管理、自定义属性管理、进程端口与配置文件管理、操作审计、资源分组、对象管理、数据审计	--
	作业功能	传输文件灵活快速、Web 化脚本管理、批量高效执行	传输文件灵活快速、Web 化脚本管理、批量高效执行、作业编排		--
	运维数据平台	不适用	满足统一数据接入、可视化计算任务配置管理、运维数据存储查询	满足统一数据接入、可视化计算任务配置管理、运维数据存储查询、可视化建模管理	--
	容器管理	不适用	应用仓库、容器编排和调度服务、多环境一致性管理、	满足应用仓库、容器编排和调度服务、多环境一致性管理、	--

			多环境一致性管理、容器网络服务	多环境一致性管理、容器网络服务、容器安全服务、一体化监控和日志查询服务	
	数据挖掘	不适用		数据分析挖掘服务	--
PaaS 层	PaaS 层	统一开发框架、企业服务总线&API GateWay	统一开发框架、企业服务总线&API GateWay、免运维托管	统一开发框架、免运维托管、企业服务总线&API GateWay、SaaS 运营数据可视化	--
运维场景层	运维场景	基础运维、监控告警、任务编排、安全审计	基础运维、监控告警、任务编排、安全审计、弹性伸缩、移动运维	基础运维、监控告警、任务编排、安全审计、弹性伸缩、移动运维、CI/CD	--
性能和效率					
原子平台层	脚本执行（在 1000 台服务器上执行 uptime 命令）	<20s	<10s	<5s	--
	文件分发（传输 500MB 文件至 1000 台服务器传输耗时）	<300s	<240s	<180s	
	DataFlow 实时计算延迟（数据平台）	<60s	<30s	<5s	
	运维数据存储查询（数据平台）	<10s	<5s	<1s	
PaaS 层	ESB 支持并发数（4 核 8G）	>16	>100	>400	
	部署单个 SaaS 平均耗时（4 核 8G）	<60s	<30s	<15s	
可靠性和可维护性					
IaaS 管控层/原子平台层/PaaS 层/运维场景层	架构高可用	存储层架构高可用	存储层、接入层架构高可用	存储层、接入层、逻辑层架构高可用	
IaaS 管控层/原子平台层/PaaS 层/运维场景层	平台服务器断电重启后的恢复情况	不适用	自动启动平台服务		--

附 录 B

（规范性附录）

云计算运维平台建设解决方案能力分级

解决方案	场景	技术要求			备注
功能					
自动化	发布	CMDB、作业功能、资源编排			--
	变更	CMDB、作业功能、资源编排			--
	故障处理	CMDB、作业功能、资源编排、监控告警			--
DevOps	持续集成(CI)	代码管理(原子层)、代码构建(原子层)、测试工具(原子层)、代码集成(原子层)			
	持续交付（CD）	代码管理(原子层)、代码构建(原子层)、测试工具(原子层)、代码集成(原子层)			
	持续部署（CD）	代码管理(原子层)、代码构建(原子层)、测试工具(原子层)、代码集成(原子层)、作业功能、资源编排			
能力指标		S1	S2	S3	
自动化	通过平台完成发布的比率	>60%	>80%	>95%	
	通过平台完成变更的比率	>60%	>80%	>95%	
	通过平台完成故障处理的比率	>60%	>80%	>95%	
	通过平台处理日常运维需求的比率	>60%	>80%	>95%	
DevOps	部署频率（将代码部署到生产环境的次数）	＞ 1 次/周	＞ 1 次/3 天	＞ 1 次/天	
	部署周期（将代码部署到生产环境的时间）	＜ 1 周	＜ 2 天	＜ 1 小时	
	部署失败率（将代码部署到生产环境失败的比率）	＜ 25%	＜ 15%	＜ 10%	
	平均故障恢复时间（服务故障后的平均恢复时间）	＜ 4 小时	＜ 2 小时	＜ 1 小时	