ICS
CCS

团　　体　　标　　准

T/COSOCC XXXX—XXXX

信息技术应用创新 云计算基础设施即服务（IaaS）通用技术要求

Information technology application innovation—General technical requirements for cloud platform Infrastructure as a Service(IaaS)

（征求意见稿）

（本草案完成时间：2023.11.24）

在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上。

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

中国基本建设优化研究会　　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。

本文件由中国基本建设优化研究会提出并归口。

本文件起草单位：

本文件主要起草人：

引　言

随着虚拟化技术与云计算、存储、网络设备等不断发展和融合创新，信息技术应用创新云计算基础设施即服务（IaaS）产品日益趋向成熟。IaaS是云计算的底座，支撑其上基础软件、应用软件、业务系统运行，是保障云计算供应链安全、稳定运行的关键。目前我国重点行业用户上云用云主要集中在IaaS层，且IaaS类产品是云计算独有核心环节。结合当前行业信息技术应用创新应用升级替代的大背景，越来越多的行业经营机构、政企机构把云计算基础设施应用于业务系统中。然而目前各方搭建的云计算基础设施在接口、框架、功能等方面不统一，给客户在选择供应商、项目验收等方面造成了困惑，同时各云计算基础设施不统一造成信息和数据不流通、接口兼容等问题，造成资源浪费。

本文件旨在提供一套完整、安全、可参考、可落地的云平台通用技术要求，提高行业内各参与方对信息技术应用创新云计算IaaS的理解，在满足行业实时性、安全性、符合监管要求的前提下，助力云计算IaaS在行业大规模推广。

信息技术应用创新 云计算基础设施即服务（IaaS）通用技术要求

1 范围

本文件规定了云计算基础设施即服务（IaaS）的总体架构以及服务器虚拟化、虚拟化云平台、云管理平台软件和桌面云的软件要求，针对不同云应用从功能性、安全性、可用性、性能效率、兼容性方面提出了相关要求。

本文件适用于信息技术应用创新云平台的设计、建设和运营，其他应用平台可参考使用。

2 规范性参考文件

本文件没有规范性引用文件。

3 术语和定义

下列术语和定义适用于本文件。

3.1

保密性 confidentiality

信息对未授权的个人、实体或过程不可用或不泄露的性质。

[来源：GB/T 25069—2022，3.41]

3.2

服务器虚拟化软件 server virtualization software

一种将物理服务器、存储、网卡等硬件，通过虚拟化技术虚拟成为多个虚拟硬件资源的软件。

注：区别于虚拟化云平台，服务器虚拟化软件最大的特点是资源利用率高，成本低，最小能支持基于单台服务器部署，通常不需要提供多租户管理、按需自助服务以及资源度量等云平台能力。

3.3

虚拟机 virtual machine

一种虚拟的数据处理系统，是在某个特定用户的独占使用下，但其功能是通过共享真实数据处理系统的各种资源得以实现的。

[来源：GB/T 35293—2017，3.1]

3.4

物理机 physical machine

相对于虚拟机的物理服务器，可为虚拟机提供硬件环境。

3.5

虚拟机管理器 hypervisor

一种在计算机硬件层上面的软件抽象层，将计算机硬件虚拟分割成一个或多个虚拟机，并提供多用户对物理计算机的访问。

[来源：GB/T 35293—2017，3.2]

3.6

虚拟资源池 virtual resource pool

一组物理资源或一组虚拟资源的集合，可从池中获取资源，也可将资源回收到池中。

注：资源包括物理机、虚拟机、物理存储、虚拟机存储、虚拟网络设备、物理网络设备等。

[来源：GB/T 35293—2017，3.3]

3.7

虚拟资源管理平台 virtual resource management platform

可以将分散的硬件资源统一起来以创建虚拟化的共享动态平台，同时实现应用程序的内置可用性、安全性和可扩展性。

[来源：GB/T 35293—2017，3.4]

3.8

虚拟机安全组 virtual machine security group

IP 过滤的规则集合，主要用于对虚拟机网络访问的控制，这些规则规定了虚拟机应该开放或阻塞的端口、网络流量类型等事项，一个虚拟机可同时属于一个或多个虚拟机安全组。

[来源：GB/T 35293—2017，3.10]

3.9

虚拟机镜像 virtual machine image

虚拟机对应的文件系统镜像，包括操作系统及虚拟机运行需要的软件。

[来源：GB/T 35293—2017，3.5]

3.10

虚拟机模板 virtual machine template

配置虚拟机所需的元数据集合，包括 CPU 数量、内存大小和存储媒体大小等。

注：虚拟机模板用于方便地生成虚拟机。

[来源：GB/T 35293—2017，3.6]

3.11

虚拟机克隆 virtual machine clone

对原始的虚拟机完全独立的一个复制，不与原始的虚拟机共享任何资源，可独立运行。

[来源：GB/T 35293—2017，3.8]

3.12

虚拟机快照 virtual machine snapshot

某时刻虚拟机状态的记录。

注：虚拟机快照用于捕获正在运行的虚拟机的状态、硬件配置等，并在需要时基于虚拟机还原到该时刻状态。

[来源：GB/T 35293—2017，3.9]

3.13

虚拟机备份 virtual machine backup

虚拟机在某时刻的信息和数据实体的副本。

注：虚拟机备份用于保存虚拟机在某时刻的状态，并在需要时用于还原到该时刻虚拟机的状态。

[来源：GB/T 35293—2017，3.7]

3.14

虚拟机热迁移 virtual machine live mig gration

通过一定的方式将实时运行的虚拟机在不关闭虚拟机的情况下从一台物理服务器迁移到另一台物理服务器上的迁移方式。

3.15

虚拟机容灾 virtual machine disaster recovery

在相隔较远的两地，建立两套或多套服务器虚拟化软件，当一处因意外（如火灾、地震等）停止工作时，整个业务系统可切换到另一处，使得该系统承载的业务正常运行。

3.16

虚拟计算资源动态调度 dynamic scheduling of virtual computing resource

一种机制，采用智能负载均衡调度算法，通过周期性检查同一集群或资源池内各个主机的计算资源负载情况，在不同的主机间迁移虚拟机。

3.17

动态电源管理 dynamic power management

一种机制，通过周期性地检查集群或资源池中服务器的资源使用情况，动态地对主机进行上/下电操作。

3.18

可用性 availability

在规定时刻或规定时间段内，部件或服务执行要求功能的能力。

[来源：GB/T 35293—2017，3.11]

3.19

整机迁移 the whole virtual machine migration

将源物理主机上指定的处于运行态的非共享存储虚拟机迁移到另外一台物理主机上，以实现不同存储媒体上虚拟机在不同节点之间迁移，迁移过程中无需中断虚拟机上的业务。

3.20

精简配置 thin provisioning

指系统首次仅分配存储媒体容量配置值的部分容量，后续根据使用情况，逐步进行分配，直到分配总量达到存储媒体容量配置值为止。

3.21

厚置备配置 thick provisioning

根据存储媒体容量为存储媒体分配空间，在创建过程中会将物理设备上保留的数据置零。

3.22

厚置备延时置零配置 thick provisioning lazy zeroed

根据存储媒体容量为存储媒体分配空间，但不会擦除物理设备上保留的任何数据，但后续从虚拟机首次执行写操作时会按需要将其置零。

3.23

虚拟机亲和 affinity

把特定的一组虚拟机调度到同一台物理机上，实现就近部署，增强网络能力实现通信上的就近路由，减少网络的损耗。

3.24

虚拟机反亲和 anti-affinity

出于高可靠性考虑，在虚拟机动态迁移的过程中尽量分散实例。

3.25

容器技术 container

寄宿于操作系统的一组进程，为应用提供相互隔离的的运行环境。

3.26

桌面云 desktop cloud

一种基于云计算的桌面交付模式。

注：在该模式下，通过将计算机桌面进行虚拟化，把个人计算环境集中存储于数据中心，为用户提供按需分配、快速交付的桌面。用户使用终端设备通过网络访问该桌面。

3.27

虚拟桌面 virtual desktop

一种基于虚拟化技术所提供的桌面应用。

注：虚拟桌面支持用户使用终端设备进行交互操作，以获得与传统个人计算机一致的用户体验。

3.28

桌面虚拟化 desktop virtualization

一种基于服务器虚拟化，并允许用户远程访问桌面并进行输入输出操作的技术。

3.29

瘦终端 thin client

一种基于虚拟化技术，使用处理器、裁剪后的操作系统，可实现对传输协议解码、显示和信息输入，为用户提供虚拟桌面交付的终端设备。

3.30

胖终端 thick client

一种具备通用处理器、本地硬盘、通用操作系统，并可安装虚拟桌面客户端软件的终端设备。

示例：传统个人计算机和便携计算机。

4 缩略语

下列缩略语适用于本文件。

API：应用程序编程接口（Application Programming Interface）

ARP：地址解析协议（Address Resolution Protocol）

BIOS：基本输入输出系统（Basic Input Output System）

CPU：中央处理器（Central Processing Unit）
GPU：图像处理器(Graphics Processing Unit)
HA：高可用性（High Availability）
HTTPS：安全超文本传输协议（Hyper Text Transfer Protocol Over Secure Socket Layer）
IO：输入/输出（Input/Output）
IOPS：每秒输入/输出操作次数（Input/Output Operation Per Second）
IP：互联网协议（Internet Protocol）
IPv6：互联网协议第6版（Internet Protocol version 6）
iSCSI：互联网小型计算机系统接口（Internet Small Computer System Interface）
MAC：媒体访问控制（Media Access Control）
NUMA：非统一内存访问（Non Uniform Memory Access）
NVME-oF：基于网络的非易失性内存快速存储访问（Non-Volatile Memory Express over Fabrics）
OS：操作系统（Operating System）
P2V：物理到虚拟（physical to virtual）
PCI：外设部件互联（Peripheral Component Interconnect）
pCPU：物理CPU（physical CPU）
QoS：服务质量（Quality of Service）
SAN：存储区域网络（Storage Area Network）
SNMP：简单网关监控协议 （Simple Network Management Protocol）
SSD：固态盘（Solid State Disk）
TLS：安全传输层协议（Transport Layer Security）
UDP：用户数据报协议（User Datagram Protocol）
UEFI：统一的可扩展固件接口（Unified Extensible Firmware Interface）
USB：通用串行总线（Universal Serial Bus）
vCPU：虚拟CPU（virtual CPU）
VLAN：虚拟局域网(Virtual Local Area Network)
vNUMA：虚拟NUMA(virtual NUMA)
VPN：虚拟专用网络(Virtual Private Network)

5 总体架构

云计算处于下层硬件基础设施和上层用户终端之间，由下往上依次由IT硬件设备、对IT资源进行池化及管理的基础设施即服务（IaaS，包括服务器虚拟化、虚拟资源调度管理、容器及调度、云管理等关键技术和产品等）、提供应用开发和运行支撑的平台即服务（PaaS，如应用开发平台、数据库、中间件等）、面向用户使用的软件即服务（SaaS，如办公系统、财务系统、ERP等）构成。

从目前IaaS产品形态来看，主要包括：

a) 支撑用户将物理机上的应用迁移到虚拟机实现业务上云的服务器虚拟化软件；
b) 实现计算、存储、网络等物理及其虚拟资源调度和控制的虚拟化云平台软件；
c) 支持用户对原有业务系统进行轻量化改造并满足快速部署和灵活调度需求的容器云平台软件；
d) 对不同云平台进行纳管，通过统一的云管平台对已建云平台和待建的不同技术路线云平台进行统一管理，实现自动化部署、配置管理等功能。
e) 通过桌面的终端设备来访问云端的应用程序或者访问云端整个虚拟桌面的桌面云产品。

IaaS产品架构示意图见图1。

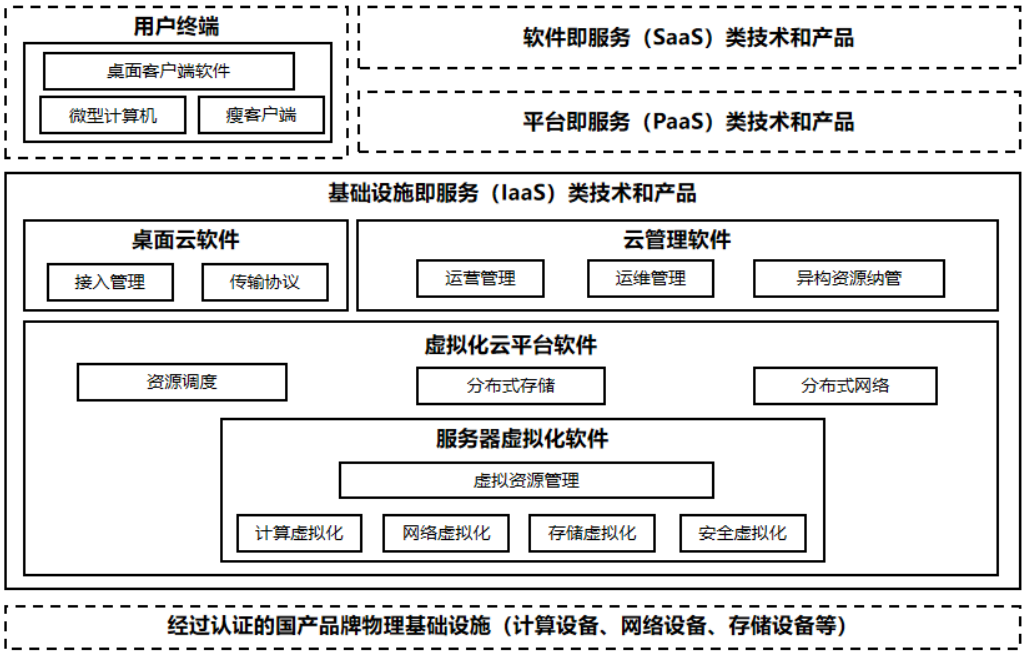

图1　云平台 IaaS 产品架构示意图

6　服务器虚拟化软件要求

6.1　功能要求

6.1.1　虚拟资源池要求

虚拟资源池要求如下：

a）　应支持物理集群、单节点的信息统计查看；
b）　应支持物理集群中增加、删除物理节点；
c）　应支持平台创建、编辑、删除多个集群，包括且不限于同类或异构 CPU 集群；
d）　应支持虚拟机集群中增加、删除虚拟机；
e）　应支持虚拟计算、存储、网络等资源池的创建、修改、信息统计查看；
f）　应支持资源池（或集群）内动态资源调度能力；
g）　应支持资源池（或集群）内动态资源扩展能力；
h）　宜支持物理节点统一管理，包括远程电源管理、网络管理、存储管理、状态监控等；
i）　宜支持虚拟机多种调度策略配置，例如亲和与反亲和等；
j）　宜支持系统资源自保障、HA 资源预留保障功能，例如为虚拟机预留 CPU 或内存资源；
k）　宜支持动态电源管理；
l）　可支持持续检测物理网卡状态。

6.1.2　虚拟化计划要求

虚拟化计划要求如下：

a）　应支持虚拟机 vCPU 与物理机 pCPU 绑定；
b）　应支持 vCPU 线程分配，为虚拟机配置指定的 CPU 槽位数、核心数；
c）　应支持 CPU、内存超分率设定；
d）　应支持裸磁盘映射，为虚拟机分配已有的虚拟或物理磁盘，以裸磁盘方式挂载；
e）　应支持物理网卡 SR-IOV 直通及虚拟化共享功能；

f） 宜支持 CPU QoS 控制功能，设置 CPU 上限/份额/预留控制能力；
g） 宜支持内存 QoS 控制功能，设置内存上限和控制功能；
h） 宜支持内存回收机制，实现虚拟化平台内存资源的动态复用；
i） 宜支持内存大页功能，虚拟机创建时支持配置指定大页规格；
j） 宜支持内存预占功能，虚拟机内部申请内存无额外性能开销；
k） 宜支持 vNUMA，虚拟机直接透传关联物理机 pNUMA 节点拓扑。

6.1.3 计算功能要求

6.1.3.1 虚拟机生命周期管理

虚拟机生命周期管理要求如下：
a） 应支持通过选择 CPU、内存、磁盘、操作系统、网络等参数创建虚拟机；
b） 应支持启动、关闭、重启、删除虚拟机；
c） 应支持虚拟机 tools 管理操作，包括安装、卸载、更新；
d） 应支持虚拟化平台访问管理虚拟机控制台；
e） 应支持虚拟机信息的查看，例如虚拟机状态、所属用户、创建时间等；
f） 应支持虚拟机启动管理操作，支持 BIOS、UEFI 等启动项配置，并指定启动顺序；
g） 应支持停机状态下虚拟机配置变更，例如 CPU 核数、内存等；
h） 应支持虚拟机初始化自定义信息（IP、网关、主机名等）注入；
i） 应支持重命名虚拟机；
j） 应支持虚拟机导入导出；
k） 宜支持至少一种方式安装部署虚拟机，例如虚拟光驱、网络引导等；
l） 宜支持虚拟机运行时 CPU、内存、磁盘的动态调整；
m） 宜支持强制关闭、重启虚拟机；
n） 宜支持重装虚拟机操作系统；
o） 宜支持虚拟机克隆、迁移、挂起、恢复、快照、备份等功能；
p） 宜支持在线修改虚拟机 GuestOS 密码；
q） 宜支持虚拟机网卡流量 QoS 控制；
r） 宜支持虚拟机存储媒体 QoS 控制；
s） 可支持创建 CPU 独占的虚拟机；
t） 可支持删除虚拟机进入回收站，并支持从回收站进行恢复；
u） 可支持批量操作多个虚拟机，例如创建、删除、暂停、恢复、关闭虚拟机等。

6.1.3.2 模板管理

模板管理要求如下：
a） 应支持对虚拟机模板创建、编辑（修改名称、描述等）、删除、查看操作；
b） 应支持基于虚拟机模板批量创建虚拟机；
c） 应支持按要求搜索已存在的虚拟机模板；
d） 应支持虚拟机模板导入导出；
e） 宜支持至少两种及以上格式的虚拟机模板跨平台导入，例如 ovf、raw、qcow2 等；
f） 宜支持虚拟机与虚拟机模板之间进行相互转换，包括虚拟机转换为虚拟机模板、虚拟机模板转换为虚拟机；
g） 可支持模板镜像的权限管理。

6.1.3.3 迁移管理

迁移管理要求如下：
a） 应支持虚拟机停机迁移和在线热迁移；
b） 应支持同指令集虚拟机业务集群统一迁移；
c） 应支持在不同品牌，架构存储上运行的虚拟机之间的迁移；
d） 应支持虚拟机在不同品牌，架构，版本的虚拟化平台间迁移；

e） 应支持在线设置迁移期间占用的磁盘 I/O，网络带宽；
f） 应支持记录虚拟机迁移日志，例如迁移任务开始时间、完成时间、迁移对象、操作者等；
g） 应设置迁移回退机制，可支持回退至迁移前的业务主机状态；
h） 应支持同芯片组架构下的裸物理服务器之间的整体迁移；
i） 可支持批量虚拟机迁移，多个虚拟机同时并发迁移；
j） 可支持跨物理主机，虚拟机等架构迁移，在线设置迁移目标机的配置信息。

6.1.3.4 快照管理

快照管理要求如下：
a） 应支持根据虚拟机创建、删除快照；
b） 应支持通过快照还原虚拟机、虚拟卷；
c） 应支持在不影响虚拟机正常运行情况下创建不带内存或带内存虚拟机快照；
d） 宜支持通过快照生成新的虚拟机或虚拟卷；
e） 宜支持对虚拟机快照进行编辑，例如修改名称、描述等；
f） 宜支持不同参数设置快照策略，例如快照执行时间、快照执行周期、快照保留策略等。

6.1.4 存储功能要求

存储功能要求如下：
a） 应支持创建、删除虚拟卷；
b） 应支持挂载、卸载虚拟卷；
c） 访问外部存储应支持 FC、iSCSI、NFS 基础存储协议；
d） 应支持虚拟存储媒体精简配置、厚置备配置或厚置备延时置零配置；
e） 宜支持 NVMe-oF 等标准协议；
f） 宜支持冷、热扩容虚拟卷；
g） 可支持虚拟卷批量创建、删除；
h） 可同时支持本地存储、集中式存储和分布式存储。

6.1.5 网络功能要求

网络功能要求如下：
c）应支持安全组创建、修改、删除、绑定、解绑；
d）应支持安全组规则添加、修改、删除；
e）应支持网络端口组策略，例如：VLAN策略；
a）宜支持虚拟私有网络IP或虚拟子网IP地址管理功能，包括创建、删除、修改、查询；
b）宜支持浮动IP创建、释放、绑定、解绑；
f）宜支持查看网络拓扑；
g）宜支持创建、修改、查询、删除网络负载均衡及路由规则等功能；
h）宜支持IPv4、IPv6双栈网络；
j）宜支持虚拟私有网络（VPC）功能，例如虚拟路由器、虚拟负载均衡、虚拟交换机、NAT网关、分布式虚拟交换机、VPC网络拓扑等；
k）宜支持组播能力；
l）宜支持创建、删除、修改、查询VPC路由；
i）可支持虚拟机共享浮动IP。

6.1.6 设备虚拟化支持功能要求

设备虚拟化支持功能要求如下：
a）应支持virtio前后端设备框架，包括不限于virtio-blk/virtio-scsi/virtio-net设备；
b）应支持USB设备直通；
c）宜支持USB设备重定向功能；
d）可支持虚拟设备信息采集，例如CPU、网卡、硬盘等。

6.1.7 运维管理要求

6.1.7.1 虚拟化指标监控要求

虚拟化指标监控要求如下：

a）应支持查看虚拟机的CPU、内存、IO等监控指标；
b）应支持查看虚拟机的存储资源、网络使用情况等监控指标；
c）应支持查看物理机CPU、内存、存储资源以及CPU利用率、内存利用率、磁盘利用率等监控指标；
d）应支持查看虚拟化平台整体CPU、内存、存储、网络等监控指标；
e）宜支持按集群或区域进行监控，包括集群内主机/虚拟机的运行状态等；
f）宜支持各类历史监控指标数据的统计分析；
g）可支持计算、存储、网络的统计报表导出（如虚拟机资源）；
h）可支持监控指标进行推或拉的操作API；
i）可支持虚拟机运行监控策略，例如故障告警等。

6.1.7.2 告警功能要求

告警功能要求如下：

a）应支持告警基本功能，包括告警上报、告警清除、告警更新等；
b）应支持告警规则配置，例如创建、编辑、删除、查询等；
c）应支持对告警规则的启用、停用；
d）应支持配置资源告警阈值（CPU、内存、存储容量、网络流量等指标）；
e）宜支持多种告警处理方式，例如告警统计、告警屏蔽、告警订阅、告警查询、告警等级设置、告警转储、历史告警导出等；
f）宜支持至少一种方式采集、推送告警信息，例如邮件、短信、SNMP、webhook等；
g）宜支持告警去重、聚合。

6.1.7.3 日志管理要求

日志管理要求如下：

a）应支持查看操作记录的日志，例如操作用户、操作名称、操作时间、执行结果、失败原因等信息；
b）应支持与第三方日志审计系统对接，例如Syslog协议、API接口等；
c）宜支持至少一种日志导出方式，例如平台下载日志、API查询导出、数据流方式导出等；
d）宜支持对操作日志设置不同的访问权限；
e）宜支持按不同属性自定义检索日志，例如时间范围、关键字等；
f）宜支持日志保留策略，满足监管日志留存要求。

6.1.7.4 虚拟机管理器运维要求

虚拟机管理器运维要求如下：

a） 应支持物理机的维护状态管理，设置维护状态的物理机将不再承载虚拟机；
b） 宜支持批量自动化安装多个虚拟化管理器；
c） 宜支持界面化一键安装部署，且可查看具体任务进展状态；
d） 宜支持无缝升级，例如在线、离线升级；
e） 宜支持虚拟化平台升级回退或回滚，升级回退过程中不中断业务；
f） 宜支持安全漏洞补丁能力；
g） 宜支持关键组件升级能力。

6.1.8 安全虚拟化

6.1.8.1 身份鉴别

身份鉴别要求如下：

a） 应支持除用户名密码外的至少一种其他身份鉴别措施，例如 UKey、动态口令等；

b） 应支持身份鉴别信息保护措施，保证传输、存储的机密性、完整性，例如要求身份鉴别信息加密存储等；
c） 应支持身份鉴别失败处理措施；
d） 应支持对密码强度、有效期、连接超时等限制设置；
e） 应支持平台登录限制，例如限制登录超时时间、网络地址等方式；
f） 应支持空闲操作超时限制功能，例如自动断开会话或重新鉴别；
g） 应支持至少一种统一认证方式，例如 LDAP、CAS、OAuth2、OIDC 等主流协议；
h） 宜支持禁止同一用户多会话连接的功能。

6.1.8.2 访问控制

访问控制要求如下：
a） 应支持通过 HTTPS 等安全协议访问平台管理服务；
b） 应支持基于角色的访问控制，例如三员分立；
c） 应支持细粒度访问控制策略设置，例如角色、用户、资源等权限设置；
d） 应支持用户资源访问行为审计；
e） 宜支持配置登录 IP 黑白名单。

6.1.8.3 用户数据保护

用户数据保护要求如下：
a）应支持身份鉴别信息的存储和传输具备加密等数据保护措施；
b）应支持虚拟机迁移过程中数据通信采用加密等数据保护措施；
c）应支持采用通信加密等方式远程管理虚拟机；
d）可支持虚拟机存储媒体清零删除。

6.1.8.4 虚拟机管理器安全

虚拟机管理器安全要求如下：
a） 应支持物理资源与虚拟机资源安全隔离功能；
b） 应支持虚拟机管理器连接鉴权，例如用户名密码、公私钥等；
c） 应支持安全组或防火墙策略；
d） 应支持配置 ACL；
e） 应支持针对一组或几组虚拟机配置相同的防火墙策略；
f） 应支持网络 bypass 功能，及与拦截日志过滤；
g） 应支持支持东西/南北向四层网络隔离，提高数据中心内部网络安全；
h） 应支持对服务器虚拟化的南北向流量镜像进行分析及风险预测；
i） 应支持对接 KMS，并使用 KMS 中的密钥加密虚拟机；
j） 应支持可视化查看虚拟机防护状态；
k） 应支持安全事件告警，告警方式包括不限于邮件等；
l） 应支持安全事件总览和安全状态展示，包含显示近三个月自动处置的暴力破解和勒索病毒数、安全事件数，以及已开启虚拟机数据保护策略的虚拟机数量；
m） 应支持虚拟机隔离；
n） 应支持虚拟机勒索应急恢复；
o） 应支持威胁处置自动快照；
p） 宜支持国密算法加密关键敏感数据及完整性校验，防止关键数据被篡改；
q） 宜支持虚拟机 web 控制台通信加密；
r） 宜提供物理机的端口安全检测功能；
s） 宜支持资源删除保护策略（如二次确认、延时删除等功能），资源包括但不限制于虚拟机、虚拟卷、镜像等；
t） 宜支持回收站功能，保障资源误删后可以恢复。

6.1.8.5 虚拟化网络安全

虚拟化网络安全要求如下：

a） 应支持虚拟网络安全组策略，例如针对虚拟机东西向流量的安全防护功能等；
b） 应支持虚拟防火墙策略；
c） 应支持网络隔离；
d） 应具有安全组件的统一管理、联动分析能力。
e） 宜支持虚拟网络安全组件；
f） 宜支持防御 IP/MAC 仿冒攻击；
g） 可支持虚拟网络报文抑制，例如虚拟机禁止广播或单播报文等。

6.1.8.6 业务安全

业务安全技术要求如下：

a） 应支持操作系统、主流应用、中间件的采集和识别；
b） 应支持病毒检测扫描，并对检测到的病毒自动处置；
c） 应具备主流 Windows 和 Linux 操作系统虚拟机底层防病毒能力；
d） 应具备虚拟机终端安全能力，支持误杀文件恢复、感染文件修复；
e） 应支持 webshell 检测扫描；
f） 应支持单个攻击源或分布式攻击源的暴力破解检测以及自动处置，及暴力破解 IP 黑名单配置；
g） 应支持防暴力破解优化；
h） 应支持攻击源自动封堵、解除；
i） 应支持恶意文件检测及文件实时监控；
j） 应支持勒索诱饵防护、勒索病毒防护以及勒索攻击对抗；
k） 应支持漏洞管理。

6.2 可靠性要求

6.2.1 虚拟机存储要求

虚拟机存储要求如下：

a）应支持虚拟存储冗余机制，例如多副本冗余、多路径冗余等；
b）应支持存储容量上限预警机制；
c）宜支持虚拟机IO悬停机制，悬停期间进行IO重试。

6.2.2 虚拟机可靠性

虚拟机可靠性要求如下：

a）应支持虚拟机高可用模式，可针对整个集群或单个虚拟机进行启用、停用设置；
b）应支持虚拟机宕机或异常退出时自动恢复；
c）应支持多网卡配置静态或动态聚合，单块物理网卡故障不影响虚拟机正常运行；
d）应支持单块磁盘故障不影响虚拟机正常运行；
e）应支持物理节点故障虚拟机自动恢复。

6.2.3 虚拟机资源管理平台可靠性

虚拟机资源管理平台可靠性要求如下：

a）应支持虚拟资源管理平台高可用部署模式，例如：主备、双活等；
b）应支持控制节点（管理节点）、计算节点、存储节点、网络节点单点故障不影响虚拟化平台正常运行。

6.2.4 虚拟机备份

虚拟机备份要求如下：

a）应支持虚拟机备份基本功能，例如创建、恢复、查询、删除等；
b）宜支持定时备份、即时备份、周期性备份；
c）宜支持全量和增量备份；

d）宜支持备份任务的配置，例如自定义并发执行的备份任务数量、备份服务的负载控制等；
e）可支持本地备份数据自动同步或定时归档到异地备份服务器；
f）应支持虚拟机无代理备份；
g）宜支持虚拟机级别的持续数据保护（CDP）；
h）可支持备份服务冗余。

6.2.5 虚拟机容灾

虚拟机容灾要求如下：
a）应支持生产业务无中断的恢复计划测试验证，确保容灾策略按需演练；
b）可支持本地数据误删后，从异地备份服务器恢复本地数据；
c）宜支持多种类型的容灾策略，例如支持秒级、小时级、天级、周级等RPO设置；
d）应支持针对计划性事件、灾难性事件的容灾恢复操作；
e）应支持容灾回迁，支持增量数据回迁。

6.3 兼容性要求

6.3.1 硬件兼容性

硬件兼容性要求如下：
a）应兼容两种或以上经过国测认证的处理器；
b）应兼容至少两种符合采购标准的通用服务器；
c）宜支持多种PCI设备，例如国产网卡、GPU、AI加速卡、国密卡等。

6.3.2 物理机兼容性

物理机兼容性要求如下：
a） 应支持至少一种符合数据库采购标准的产品；
b） 宜支持至少一种符合操作系统采购标准的产品。

6.3.3 虚拟机兼容性

虚拟机兼容性要求如下：
a）应支持主流商业操作系统；
b）应支持两种或以上符合操作系统采购标准的产品。

7 虚拟化云平台软件要求

7.1 功能要求

7.1.1 资源层要求

7.1.1.1 主机管理

主机管理要求如下：
a） 应支持添加、删除主机以及主机信息查看等；
b） 应支持进入、退出维护模式。

7.1.1.2 集群管理

集群管理要求如下：
a） 应支持创建、删除主机集群，以及查看集群信息等；
b） 应支持向集群中添加、移除主机；
c） 应支持在虚拟化云平台中创建不同的集群，可以创建2个及2个以上的集群；
d） 应支持主机集群的人工配置或自动化管理，如配置集群策略，CPU负载临界值等；
e） 应支持一云多芯的不同集群纳管。

7.1.1.3 虚拟资源管理

虚拟资源管理要求如下：

a) 应支持对计算资源池、存储资源池、网络资源池的管理，包括：要求可以在云平台中对计算资源池、存储资源池、网络资源池（包括虚拟私有网络和浮动IP）进行分类管理；要求可以查看资源池相关信息，以及对资源池可用容量的监控等；
b) 宜支持存储资源池的扩容和缩容，要求支持分布式存储或集中式存储其中一种方式。

7.1.1.4 裸金属服务

裸金属服务要求如下：

a) 应支持列举平台支持的裸金属服务器规格及相关硬件配置信息；
b) 应支持申请选择裸金属服务器规格的裸机；
c) 应支持远程启动、关闭裸金属服务器；
d) 应支持获取单个裸金属服务器的详细信息；

7.1.1.5 虚拟机生命周期管理

虚拟机生命周期管理要求如下：

a) 应支持配置CPU、内存、磁盘、操作系统、网络、可用区等参数创建单台或批量虚拟机；
b) 应支持启动、重启、关闭(强制关闭、强制重启)；
c) 应支持创建时指定分布式存储、集中式存储或本地存储作为虚拟机的磁盘存储；
d) 应支持创建CPU独占或CPU共享的虚拟机；
e) 应支持删除虚拟机后，能够列举平台虚拟机规格及相关配置信息；
f) 应支持列举虚拟机信息；
g) 应支持查询指定虚拟机当前状态、虚拟机所属的用户、虚拟机创建的时间、虚拟机磁盘等信息；
h) 应支持修改虚拟机名称；
i) 应支持停机扩容CPU、内存；
j) 应支持云主机磁盘、网卡的挂载和卸载；
k) 应支持从控制页面远程登录云主机；
l) 应支持多个虚拟机挂载共享磁盘；
m) 应支持不同规格的虚拟机调度，达到主机资源的负载均衡；
n) 在虚拟机操作系统支持的前提下，宜支持虚拟机资源的动态调整（包括CPU、内存、网络、磁盘等）。

7.1.1.6 虚拟机迁移

虚拟机迁移要求如下：

a) 应支持虚拟机的冷、热迁移；
b) 应支持将虚拟机磁盘从一个共享存储迁移到另一个共享存储；
c) 应支持整体迁移。

7.1.1.7 快照/克隆/备份服务

快照/克隆/备份服务要求如下：

a) 应支持虚拟机整机进行备份，如虚拟机快照、备份或克隆；
b) 应支持使用虚拟机备份恢复到原虚拟机，支持恢复到其它云主机；
c) 应支持使用云硬盘备份恢复到原云硬盘，支持恢复到其它云硬盘；
d) 应支持创建、修改、删除备份策略，如设置备份频率和备份保留规则；
e) 应支持通过设置备份策略周期性地自动备份；
f) 应支持按照清理规则自动清理备份。

7.1.1.8 镜像服务

镜像服务要求如下：

a) 应支持虚拟机镜像的新建和删除等操作；
b) 应支持虚拟机镜像信息的修改；

c） 应支持虚拟机镜像的导入、导出；
d） 应支持镜像管理，用户可以查看虚拟机镜像基本信息，包括镜像名称、操作系统、镜像文件大小等；
e） 应支持共有镜像，由管理员创建供所有用户使用；
f） 应支持私有镜像，由用户自己创建，仅供用户自己使用。

7.1.1.9 弹性伸缩服务

弹性伸缩服务要求如下：
a） 应提供弹性伸缩服务，通过设置策略自动调整资源以应对业务变化的压力；
b） 应支持根据CPU、内存资源的使用情况配置伸缩策略；
c） 应支持配置弹性伸缩服务的最大、最小可支持的虚拟机数量；
d） 应支持查看特定伸缩组里面当前的虚拟机数量、伸缩日志。

7.1.2 存储服务

7.1.2.1 块存储服务

块存储服务要求如下：
a） 应提供卷管理，包括创建卷、删除卷、查询卷、挂载卷、卸载卷、修改卷、扩容卷；
b） 应支持通过控制台查看资源使用情况、操作日志等信息；
c） 应支持卷备份的创建、删除、修改、查询、恢复，包括增量备份与全量备份；
d） 应支持卷快照的创建、删除、修改、查询、恢复；
e） 应支持对卷的批量操作，包含创建、删除；
f） 应支持使用卷的快照、备份创建卷。

7.1.3 网络服务

7.1.3.1 虚拟私有网络管理

虚拟私有网络管理要求如下：
a） 应支持创建虚拟私有网络，如：指定虚拟私有网络名称、VPC网段等参数；
b） 应支持删除虚拟私有网络，如：虚拟私有网络ID等参数；
c） 应支持私有IP地址管理功能；
d） 应支持查询虚拟私有网络实例列表，如：虚拟私有网络ID等参数；
e） 应支持修改虚拟私有网络属性，如：虚拟私有网络、VPC名称等参数；
f） 应支持查询虚拟私有网络属性，如：指定地域、虚拟私有网络等参数。

7.1.3.2 虚拟私有网络子网管理

虚拟私有网络子网管理要求如下：
a） 应支持创建虚拟私有网络子网，包括支持指定虚拟私有网络子网名称、所在地域、虚拟私有网络ID、可用区、子网网段、是否使能IPv6等参数；
b） 应支持删除虚拟私有网络子网；
c） 应支持查询虚拟私有网络实例子网列表，如：指定地域、虚拟私有网络ID、虚拟私有网络子网ID等参数；
d） 应支持修改虚拟私有网络子网属性，如指定地域、虚拟私有网络ID、子网ID、子网名称；
e） 应支持查询虚拟私有网络属性，如指定地域、虚拟私有网络ID、子网ID等参数查询；
f） 应支持配置子网静态路由，如配置子网静态路由、修改子网静态路由、删除子网静态路由。

7.1.3.3 虚拟路由规则管理

虚拟路由规则管理要求如下：
a） 应支持添加路由规则，如指定目标网段，下一跳地址，路由表ID，优先级等信息添加路由表；
b） 应支持修改虚拟路由属性，如指定路由器ID修改虚拟路由器描述及名称；

c） 应支持删除路由规则，如指定目标网段，下一跳地址，路由表ID、路由规则ID、等信息删除路由表；
d） 应支持查询路由规则，如指定目标网段、路由表ID、路由规则ID等信息宜支持修改路由规则，如可修改路由条目名称。

7.1.3.4 公网 IP 服务

公网IP服务要求如下：
a） 应支持分配公网IP；
b） 应支持绑定、解绑公网IP到云产品实例；
c） 应支持查询公网IP列表；
d） 应支持修改公网IP属性；
e） 应支持释放公网IP。

7.1.3.5 NAT 网关服务

应支持创建、修改、查询、删除NAT网关服务。

7.1.3.6 VPN 服务

应支持创建、修改、查询、删除VPN服务。

7.1.3.7 负载均衡服务

负载均衡服务要求如下：
a） 应支持负载均衡器的创建、删除、修改、查询；
b） 应支持负载均衡器对后端资源的挂载、卸载；
c） 应支持实时监控负载均衡器运行状态；
d） 应提供多种负载均衡策略；
e） 应支持负载均衡配置的下发、负载均衡配置信息的修改；
f） 应支持浮动IP模式（挂载在负载均衡器的外网IP）；
g） 应支持提供四层（TCP协议和UDP协议）和七层（HTTP和HTTPS协议）的负载均衡服务；
h） 应支持负载均衡集群高可用能力；
i） 应支持后端虚拟机健康检查能力。

7.1.4 管理服务

7.1.4.1 资源编排服务

资源编排服务要求如下：
a） 应支持创建资源编排模版，支持对编排模版增删改查等管理；
b） 应支持通过模板发放云资源和部署实例；
c） 应支持图形化模板工具要求通过界面方式将多种服务编排组合。

7.1.5 组织管理

7.1.5.1 账号管理

账户管理要求如下：
a） 应支持租户资源隔离，不同租户只能管理自己的资源，管理员可以管理所有资源；
b） 应支持租户下的用户组管理；
c） 应支持以资源组为粒度进行云资源管理；
d） 应支持多级资源组管理；
e） 应支持每级资源组设置一个或者多个独立的管理员；
f） 应支持按照资源组维度对资源组内所有用户的操作日志进行汇总，可以按照不同维度进行过滤，实现安全审计。

7.1.5.2 配置管理

应支持按照资源组进行资源配额管理。

7.1.6 用户管理

用户管理要求如下：

a) 应支持用户的创建、修改、删除、查询，启用/禁用；
b) 应支持按照资源组定义角色,至少包括资源组管理员与资源组用户；
c) 应支持按照角色为用户分配权限；
d) 应支持按云服务自定义角色权限；
e) 应支持统一身份认证；
f) 应提供用户登录，退出等运营日志。

7.1.7 计量管理

7.1.7.1 计量管理

计量管理要求如下：

a) 应支持对租户的资源使用量进行统计；
b) 应支持对计算资源按照规格或CPU、内存进行计量，计量周期至少以小时为单位；
c) 应支持按照虚拟资源组、资源组维度进行统计；
d) 应支持计量数据的导出；
e) 应支持费用明细清单。

7.1.7.2 订单管理

应支持订单管理，包括申请、审批、查询等。

7.1.7.3 审批流程管理

审批流程管理要求如下：

a) 应提供虚拟机、存储和虚拟私有网络等服务的申请、审核以及开通等功能，租户可在云平台上进行虚拟机、存储、虚拟私有网络以及负载均衡等服务的申请、审核、开通等；
b) 应提供批量申请功能，租户可在云平台上同时申请3个及以上的虚拟机、存储服务；
c) 应提供自助扩容（包括计算资源、存储资源、网络资源）等功能，租户可以在云平台上提出扩容申请；
d) 应支持服务的自动审批/免审批、支持服务审批后自动部署。

7.1.8 服务目录管理

服务管理目录要求如下：

a) 应支持服务/产品目录统一浏览；
b) 应支持查阅各项服务/产品信息；
c) 应支持服务/产品目录中服务/产品的生命周期管理，包括发布、修改、卸载、查找、下线等。

7.1.9 服务访问管理

服务访问管理要求如下：

a) 应支持通过远程方式访问虚拟机，虚拟机的远程连接应通过云平台界面进行；
b) 应支持通过Web方式访问云平台；
c) 在业务支撑层面应支持单点登录控制。

7.1.10 告警管理

告警管理要求如下：

a) 应支持告警事件管理，如告警阈值设置、告警通知、告警查询；
b) 应支持告警原因的展示。

7.1.11 监控管理

7.1.11.1 资源监控

资源监控要求如下：

a) 应支持监控设置；
b) 应支持按集群进行监控，包括集群内主机/虚拟机的运行状态等；
c) 应支持主机资源监控，包括CPU、存储、网络、内存；
d) 应支持虚拟资源监控，对虚拟机资源进行监控，以图形化界面或统计报表方式显示；
e) 应支持租户对其所拥有资源的监控，包括计算资源、存储资源、网络资源；
f) 应虚拟机网络状态监控，包括虚拟机网卡的流量统计与网络安全组展示；
g) 应支持实时监控（支持60秒及以内的监控频率）或历史监视结果可视化展现；
h) 应支持监控数据的查询、统计。

7.1.11.2 报表管理

报表管理要求如下：

a) 应支持各种资源的统计报表，包括物理主机性能统计报表、云主机性能统计报表、使用统计报表、统计报表等；
b) 应支持指定时间生成报表，报表样式支持表格，曲线图，饼图，柱状图等至少一种形式，报表可以导出保存为Excel，CSV，PDF等至少一种格式。

7.1.12 日志管理

日志管理要求如下：

a) 应提供云资源申请，变更，释放等运营日志；
b) 应支持按时间、操作人、事件、IP地址等信息对运营日志进行过滤；
c) 操作日志宜记录所有类型的操作员（含系统管理员、租户管理员、租户用户等）在系统上的操作；
d) 每条操作日志宜包含操作员、操作对象、操作类型、操作描述、操作时间、操作结果等信息。

7.1.13 配置管理

配置管理要求如下：

a) 应支持配置数据的备份与恢复；
b) 应支持对平台进行巡检，以便及时发现问题和风险；
c) 应巡检的内容宜包括云平台组件的运行状态等。

7.1.14 系统维护管理

系统维护管理要求如下：

a) 应支持系统组件的版本升级功能；
b) 应支持计算、存储物理资源的扩容和缩容。

7.2 虚拟化云平台安全要求

7.2.1 运维/运营身份鉴别功能

运维/运营身份鉴别功能要求如下：

a) 应提供两种及以上身份鉴别措施，不限于用户名密码、短信验证、Ukey、人物特征识别、证书等；
b) 应提供身份鉴别信息保护措施，身份信息应加密存储；
c) 应提供鉴别失败处理措施；
d) 应提供禁止同一用户多会话连接的功能；
e) 应支持对密码强度、有效期、服务等限制设置
f) 整个生命周期内用户标识宜唯一（运维涉及角色包括管理员、运维人员）。

7.2.2 访问控制功能

7.2.2.1 运维访问控制功能

运维访问控制功能要求如下：

a) 应提供授权管理功能，主要针对管理员和运维人员提供读写或只读权限；
b) 应支持权限分离，要求管理员无法查看租户虚拟机内部信息；
c) 应支持细粒度访问控制策略的设置。

7.2.2.2 运营访问控制功能

运营访问控制功能要求如下：

a) 应提供针对租户的授权管理功能；
b) 应支持权限分离。要求租户无法查看其他租户的内部资源；
c) 应支持细粒度访问控制策略的设置；
d) 应支持虚拟机防ARP欺骗，如采用IP地址和MAC地址绑定的方式；
e) 应支持虚拟机迁移后安全组策略不变。

7.2.2.3 多用户身份类型功能

多用户身份类型功能要求如下

a) 应为用户提供用户身份管理与访问控制服务；
b) 应支持创建、管理用户账号，并可以分配这些账号对其名下资源具有的操作权限。

7.2.2.4 权限隔离功能

应支持对资源管控类和资源使用类操作的权限管理。

7.2.3 存储加密

存储加密要求如下：

a) 应支持对运维日志、客户操作日志等数据进行保护，可以采用加密处理等方式；
b) 应支持客户部署数据加密方案，确保客户的数据能够在云平台以密文形式存储；
c) 应支持用户自选密钥功能，允许用户上传密钥并对数据进行加密，并允许用户在密钥生命周期内进行全程管理。

7.2.4 传输加密

应确保数据传输过程的保密性，可使用VPN、HTTPS等传输方式。

7.2.5 事件日志记录

事件日志记录要求如下：

a) 应对账号登录、账号管理、系统事件、对虚拟化平台的操作等行为进行日志记录；
b) 应日志记录内容至少包括事件类型、事件发生的时间事件来源、事件结果以及与事件相关的用户或主体的身份；
c) 应保证云平台内部和用户相关的操作事件对用户可见，允许用户进行审计监控。

7.2.6 虚拟机保护

虚拟机保护要求如下：

a) 应支持虚拟机隔离，保证虚拟机之间的安全隔离，保护CPU、内存和存储空间安全隔离；
b) 应提供虚拟机与主机间网络隔离；
c) 应提供云平台的补丁更新。

7.3 可靠性要求

可靠性要求如下：

a) 主机出现故障时，虚拟机应具备HA能力；
b) 主机出现故障时，虚拟机应可进行故障恢复；
c) 宜支持单个存储节点出现故障时，不影响虚拟化云平台正常运行，并保证数据的一致性；

d) 宜支持存储节点的网络可用性，当冗余网络中的一个网络链路中断时，不影响虚拟化云平台正常运行，并保证数据一致性；
e) 宜支持单台控制节点/存储节点/网络节点出现故障，平台仍可正常使用。

7.4 兼容性要求

7.4.1 硬件兼容性

硬件兼容性要求如下：
a) 宜支持计算和控制节点为自主芯片的服务器；
b) 宜兼容自主存储设备；
c) 宜兼容自主交换机。

7.4.2 虚拟机兼容性

宜支持两种及以上国产操作系统镜像。

8 云管理平台软件要求

8.1 用户门户功能要求

8.1.1 资源申请

8.1.1.1 提交申请

应支持下列功能：
a) 在申请时可以指定产品的规格参数；
b) 在申请时可以指定产品数量；
c) 在申请时可以指定使用期限；
d) 在填写完成必要的申请参数后，用户可以立即提交申请单；
e) 在填写完成必要的申请参数后，用户可以选择保存申请单，留待后续批量提交多个已经保存的申请单；
f) 用户提交申请单后，云平台根据运营管理员或组织管理员预先配置的审批流程，将申请单提交给指定的审批人进行审批。

8.1.1.2 修改申请

应支持下列功能：
a) 用户可以查看已经提交的申请单；
b) 申请人在申请单未审批前可以撤回并再次提交；
c) 在申请单被审批人驳回时，被驳回的订单可以经申请人修改后再次提交。

8.1.1.3 查看详情

应支持用户可以查看已经提交的申请订单，跟踪订单的进行状态。

8.1.2 自动监控

8.1.2.1 资源性能

应支持下列功能：
a) 用户可分类查看已经申请到的云资源列表；
b) 用户可查看已经申请到的云资源的相关性能监控数据；
c) 云资源性能分析图表展示。

8.1.2.2 阈值管理

应支持下列功能：
a) 用户可查看已经申请到的云资源相关的告警；

b） 用户可对告警消息确认、关闭；
c） 云资源性能监控阈值管理、超过阈值设定产生相应告警；
d） 通过邮件或短信方式将云资源告警信息通知给指定的用户。

8.1.2.3 操作日志

应支持下列功能：
a） 记录用户操作日志，包括申请、变更、删除云资源，以及对云资源的操作日志记录，例如关闭、启动弹性云服务器等；
b） 用户查询自己的操作日志；
c） 组织管理员查询组织内所有用户的操作日志。

8.1.3 计量统计

用户可查看已经申请到的资源的计量统计信息。

8.1.4 计算资源

应支持下列功能：
a） 用户申请受管云平台的计算资源，例如云服务器、裸金属服务器等；
b） 用户对已经申请到的计算资源进行管理，包括变更、释放、查询操作；
c） 用户批量申请、变更、释放、查询计算资源；
d） 用户对已经申请到的计算资源进行业务操作，例如启动、关闭、重启、远程登录等。

8.1.5 存储资源

应支持用户实现下列功能：
a） 申请受管云平台的存储资源，例如弹性云硬盘、对象存储、文件存储等；
b） 对已经申请到的存储资源进行管理，包括变更、释放、查询操作；
c） 批量申请、变更、释放、查询存储资源；
d） 对已经申请到的存储资源进行相应的业务操作，例如挂载卷、卸载卷、创建目录、上传文件、下载文件等。

8.1.6 网络资源

应支持用户实现下列功能：
a） 申请受管云平台的网络资源，例如VPC、弹性IP、ELB等；
b） 对已经申请到的网络资源进行管理，包括变更、释放、查询操作；
c） 批量申请、变更、释放、查询网络资源；
d） 对已经申请到的网络资源进行相应的业务操作，例如配置子网、配置路由、绑定IP到指定虚拟机、配置负载均衡规则等。

8.2 运营门户功能要求

8.2.1 服务目录

服务目录应符合下列要求：
a） 支持计算资源、网络资源、存储资源和容器资源的服务目录管理能力；
b） 支持服务的生命周期管理能力，包括服务定义、发布、查看、变更和下线；
c） 支持服务的权限管理，控制用户对相关服务的可见范围；
d） 支持服务的流程管理，控制相关服务的申请审批流程；
e） 支持多种类资源组合的服务目录定义能力。

8.2.2 组织管理

8.2.2.1 多级组织管理

多级组织管理应符合下列要求：

a） 支持至少3级组织的增删改查的管理能力；
b） 支持同级别组织之间资源默认逻辑隔离；
c） 支持上级对其所有级联下级组织的管理能力；
d） 支持组织的变更归属能力，其组织及其所有下级组织所有资源级联变更。

8.2.2.2 资源组管理

资源组管理应符合下列要求：
a） 支持组织内的资源分组管理能力，一个组织内部可以创建多个资源组，一个资源实例只能归属于一个资源组；
b） 支持资源组之间的资源默认逻辑隔离；
c） 支持资源组的变更归属组织能力，其内部的资源实例级联变更。

8.2.3 用户管理

用户管理应符合下列要求：
a） 支持用户的增删改查能力；
b） 支持用户的登陆策略控制能力；
c） 提供用户参与到多个资源组的能力；
d） 提供用户变更所属组织的能力；
e） 支持用户的与外部系统(LDAP等)认证对接能力；
f） 支持用户的激活、禁用和删除等能力；
g） 支持用户的多因子认证及强密码策略等能力；
h） 支持用户组的增删改查能力，一个用户可以加入到多个用户组。

8.2.4 权限管理

应具备下列权限管理功能：
a） 满足基于角色的访问控制（RBAC）规范；
b） 具备预置的通用业务角色，如运营管理员、组织管理员和资源使用人等；
c） 具备角色的自定义创建和编辑能力；
d） 具备角色授予用户的能力；
e） 支持一个用户被授予多个角色；
f） 具备角色的切换能力。

8.2.5 配额管理

配额管理应符合下列要求：
a） 支持对组织级别的云资源配额的分配和调整，相关云资源的使用量不能超过配额量；
b） 支持对资源组级别的云资源配额的分配和调整，相关云资源的使用量不能超过配额量；
c） 支持从上而下的配额分配，按组织的层级逐级下放并分配配额；
d） 支持从下而上的配额回收，按组织的层级逐级上升并回收配额；
e） 支持组织和资源组的配额使用情况查看，包括本组织的配额，分配给下级的配额，和配额的已使用量等信息。

8.2.6 资源管理

应支持通过链接、用户名、密码便捷接入各类受管云资源，以受管云平台、资源域等逻辑单位进行纳管。

8.2.7 计量管理

计量管理应符合下列要求：
a） 支持时间维度的资源计量，如按小时、天和月等时间单位进行计量；
b） 支持资源状态，资源数量，以及资源用量等多方面的计量数据；
c） 支持按照组织、资源组和云服务维度的计量数据统计查看及导出；

d) 对外开放计量数据的相关接口，用于对接第三方计费系统；
e) 针对云资源的计量单位（如CPU、内存、存储、IP等）设置对应价格，并可根据时间段生成和导出统计报表。

8.2.8 流程管理

应支持下列流程管理功能：
a) 云资源实例的开通申请审批流程管理；
b) 云资源实例的配置变更申请审批流程管理；
c) 组织和资源组配额调整的申请审批流程管理；
d) 流程的自定义调整能力；
e) 自动审批流程和人工审批流程；
f) 角色权限的申请审批流程管理。

8.2.9 统计分析

应能提供以下统计分析报表并满足相应要求：
a) 云资源的统计分析报表，支持按照多维度的查询和导出能力，例如组织、资源组、服务类型等；
b) 云平台的配额使用情况的统计分析报表，支持多维度的查询和导出能力，例如按照组织、资源组、服务类型等；
c) 云资源告警的统计分析报表，支持多维度的查询和导出能力，例如按照组织、资源组、服务类型等。

8.2.10 资源编排

应支持下列资源编排功能：
a) 对多种类型的云资源进行组合编排；
b) 可视化的在线编排工具；
c) 基于编排实例的多种云资源批量创建；
d) 将资源编排的实例发布为编排模板；
e) 提供基于图形化拖拽的资源编排工具。

8.2.11 资源调度

应支持下列资源调度功能：
a) 基于资源性能告警的云资源弹性调度策略；
b) 提供基于多种维度组合指标的云资源弹性调度策略，如基于定时任务的云资源弹性调度策略；
c) 提供被纳管云存量资源的动态发现和纳管能力。

8.3 运维管理门户功能要求

8.3.1 资源监控

应支持下列资源监控功能：
a) 资源池维度监控；
b) 宿主机维度资源监控，包括CPU、内存、网络、存储；
c) 虚拟化资源实例维度监控，包括CPU、内存、网络、存储 ；
d) 查询一段时间内的多类监控指标的历史数据，并图形化展现；
e) 租户内资源监控，包括资源实例使用统计、使用趋势；
f) 对监控指标定义阈值和告警策略，实现异常状态告警；
g) 调整监控指标的采集周期。

9 桌面云软件要求

9.1 功能要求

9.1.1 虚拟桌面分配与管理

应支持下列虚拟桌面分配与管理功能：

a) 用户管理，包括用户添加、编辑、删除；
b) 进行虚拟桌面的批量管理，包括批量创建、批量开机、批量关机等，支持批量关联与解关联用户；
c) 分配虚拟桌面、回收虚拟桌面；
d) 恢复虚拟桌面或者彻底删除虚拟桌面；
e) 虚拟桌面使用情况统计。

9.1.2 虚拟桌面使用管理

应具备下列虚拟桌面使用相关的功能：

a) 支持从外部网络接入虚拟桌面；
b) 支持设置虚拟桌面连接显示策略，配置虚拟桌面连接参数；
c) 支持虚拟桌面自适应终端分辨率；
d) 支持单用户连接多个虚拟桌面；
e) 支持虚拟桌面软终端的工具栏隐藏；
f) 支持网络断开后指定时间内终端自动重连；
g) 支持多屏显示，并可实现复制或扩展两种模式；
h) 支持设置虚拟桌面协议的画质策略（如清晰度）；
i) 支持用户从客户端重启或关闭虚拟桌面。

9.1.3 应用程序使用管理

应具备下列应用程序使用相关的功能：

a) 支持管理员发布、查询、删除应用软件程序；
b) 支持应用软件资源池信息的显示，并提供可视化界面；
c) 支持在本地桌面创建远程应用程序快捷方式；
d) 支持在本地桌面通过双击远程应用程序快捷方式打开远程应用；
e) 支持本地桌面文档通过远程应用无缝打开，打开方式可为双击打开或右键关联打开；
f) 支持本地桌面剪贴板与远程应用内剪贴板的数据共享；
g) 支持配置外设使用策略，支持本地外设(U盘、打印机、高拍仪、扫描仪、摄像头等)被重定向到远程应用上；
h) 支持单实例应用发布，多用户可同时使用单实例应用；
i) 关闭服务端远程桌面服务（如Remote Desktop Service），应用程序正常运行；
j) 支持单应用多用户间的数据隔离，用户无法查看和操作其他用户的数据，且禁止超级管理员角色。

9.1.4 虚拟桌面数据交换管理

应支持下列虚拟桌面数据交换功能：

a) 虚拟桌面协议支持数据传输加密，如图形、视频、语音等数据传输的安全性；
b) 支持本地USB管控，除指定列表中USB设备外，其他USB设备均可被管控；
c) 支持本地桌面与虚拟桌面间使用剪切板功能，管理员可设置单向/双向数据传输的权限；
d) 支持将本地文件系统重定向至虚拟桌面，管理员可设置重定向后文件夹权限为只读或读写；
e) 支持剪切板文件和文字审计。

9.1.5 虚拟桌面运维管理

应支持下列虚拟桌面运维功能：

a) 虚拟桌面展现实时状态，按运行状态、登录状态、分配状态等维度统计系统中虚拟桌面资源使用情况；
b) 虚拟桌面分组管理；

c） 对虚拟桌面代理进行升级；
d） 操作日志查询和导出；
e） 虚拟桌面信息导出功能。包括虚拟机名称、虚拟机规格、分组信息、所属用户等信息；
f） 通信协议性能监控，显示虚拟桌面使用时实时网络带宽、网络延迟、丢包率；
g） 配置定时任务，包括虚拟桌面的定时开机、定时关机等；
h） 管理员对虚拟桌面创建快照、进行快照恢复；
i） 管理员授权用户对虚拟桌面自行进行快照恢复；
j） 用户、终端、虚拟桌面之间的权限绑定。

9.1.6 虚拟桌面外设管理

应支持下列虚拟桌面外设管理功能：
a） 将客户端的USB设备重定向至虚拟机，如存储类USB设备、扫描仪、打印机等；
b） 多种外设重定向策略的管理，支持针对不同的外设对象设置策略。

9.1.7 桌面网络管理

应支持下列桌面网络管理功能：
a） 虚拟桌面传输网络QoS，对网络进行上行、下行带宽限制；
b） 虚拟机网络与终端网络隔离。

9.1.8 软终端管理

应支持下列软终端管理功能：
a） 支持软终端程序升级更新；
b） 支持检查网络环境、连接设置，具备错误信息提示功能；
c） 提供屏蔽PC的桌面、开始菜单和本地资源等功能；
d） 虚拟桌面软终端支持窗口模式运行、全屏模式运行。

9.1.9 虚拟机管理

应支持下列虚拟机管理功能：
a） 对虚拟机进行创建、删除、重启、停止、启动，以及创建模板或镜像等操作；
b） 镜像的编辑和CPU、内存、磁盘等规格管理；
c） 通过虚拟机镜像模板产生链接克隆虚机；
d） 按需扩容，调整虚拟机的CPU核数、内存大小、以及磁盘容量等；
e） 按条件筛选虚拟机，并导出虚拟机列表；
f） 模板更改后统一更新到对应的虚拟机；
g） 虚拟机定时策略，虚拟机长时间无操作时，可设置定时断开连接、注销或关机；
h） 虚拟机资源（CPU、内存）监控和状态监控（在线或离线）。

9.1.10 服务器管理

应支持下列服务器管理功能：
a） 添加服务器到桌面云平台，及从桌面云平台移除指定服务器，过程中桌面云系统运行正常；
b） 对服务器进行远程操作，包含关机、重启、维护模式、配置主机网络等；
c） 主机的CPU、内存、磁盘、网络等资源监控和告警；
d） 共享存储，如IP-SAN、 FC-SAN存储；
e） 主机资源池的存储资源在线扩容；
f） 创建、删除主机集群，以及查看集群信息等；
g） 主机端口汇聚，将多个网络端口聚合；
h） 集群资源动态调度策略管理。

9.2 桌面云安全要求

9.2.1 权限管理

应符合下列权限管理要求：

a） 采用三员分立管理策略，系统应具备系统管理员，安全保密管理员，安全审计员三个独立的角色；

b） 支持限制用户按时间、网络地址等条件访问虚拟桌面。

9.2.2 接入认证安全要求

应符合下列接入认证要求：

a） 支持通过用户名和口令进行身份认证，用户认证的口令强度必须为字母、数字、特殊字符两种及以上组成；

b） 支持首次登陆强制修改密码、定期修改密码；

c） 支持在系统设定的时限范围内没有操作情况下，断开用户会话或重新鉴别用户身份；

d） 当用户认证失败达到指定次数后，系统应采取相应的措施阻止用户再次发起认证请求；

e） 禁止使用不安全协议，如HTTP方式访问；

f） 支持客户端准入检测，如根据用户接入ip、时间、终端硬件标识等访问策略，客户端不满足检测要求不允许接入。

9.2.3 数据安全

应符合下列数据安全要求：

a） 用户的身份鉴别信息在存储中加密；

b） 支持对虚拟桌面系统盘执行还原，不影响数据盘使用。

9.2.4 身份鉴别

应符合下列身份鉴别要求：

a） 整个生命周期内用户标识应唯一；

b） 提供两种及以上的身份鉴别措施，不限于用户名密码、短信验证、Ukey、人物特征识别、证书等；

c） 提供身份鉴别信息保护措施，如提供相关信息的加密存储；

d） 提供禁止同一用户多会话连接的功能；

e） 支持对密码强度、有效期、IP地址、时间、资源等限制设置。

9.2.5 访问控制

应符合下列访问控制要求：

a） 提供授权管理功能，针对运维管理员、运维人员、租户提供读写或只读权限；

b） 支持权限分离，管理员无法查看租户虚拟机内部信息，租户无法查看其他租户的资源；

c） 支持细粒度访问控制策略的设置；

d） 支持配置基于用户、虚拟机、IP地址之间的访问隔离控制；

e） 支持应用的黑白名单控制，如可以根据应用进程、应用特性信息等多维度进行管控。

9.2.6 权限隔离

应支持对资源管控和资源使用类操作的权限管理。

9.2.7 传输加密

应符合下列传输加密要求：

a） 确保数据传输过程的保密性，如采用HTTPS方式；

b） 支持对运维日志、客户操作日志等数据进行保护，可以采用加密处理等方式。

9.2.8 日志审计

应符合下列日志审计要求：

a） 对账号登录、账号管理、系统事件、对云管平台的操作等行为进行日志记录；

b） 日志记录内容至少包括事件类型、事件发生的时间事件来源、事件结果以及与事件相关的用户或主体的身份；
c） 保证云管平台内部和某用户相关的操作事件对其可见，并可进行筛选查询审计。

9.3 可靠性要求

可靠性要求如下：
a） 应管理节点采用主备方式或负载均衡方式确保平台的可用性；
b） 应支持链路聚合，拔除一根网线，业务不受影响；
c） 应虚拟桌面中的代理软件具备防卸载功能，如需卸载需要卸载密码；
d） 应支持对虚拟桌面进行增量或全量备份；
e） 应支持定期对虚拟桌面备份，并导出在其他平台存档备份；
f） 应支持虚拟桌面能够恢复到备份点的状态；
g） 应单服务器上启动5台虚拟桌面，并发负载运行7*24小时，桌面云系统无崩溃现象，虚拟桌面运行正常；
h） 宜在服务器出现故障后，支持虚拟桌面自动迁移；
i） 宜拔出某块数据盘，该主机正常运行，桌面云平台出现故障告警，虚拟机不受影响；
j） 宜支持对虚拟机指定分区进行备份、还原。

9.4 兼容性要求

9.4.1 终端操作系统兼容要求

终端操作系统应符合下列兼容性要求：
a） 应兼容至少2种不同CPU架构的终端设备；
b） 软终端软件应至少兼容2款操作系统。

9.4.2 镜像操作系统兼容性

应支持至少2款经过国测检测的操作系统。

9.4.3 外设兼容性

虚拟桌面和远程应用均应兼容U盘、打印机、高拍仪、扫描仪、摄像头、Ukey等外设。

9.4.4 利旧管理

同一套桌面云系统，应具备兼容国产服务器、国产终端，利旧x86服务器、x86终端的能力。

9.5 易用性要求

9.5.1 易访问要求

应符合下列易访问要求：
a） 提供远程应用快速访问列表，提供应用分类显示；
b） 软终端与虚拟桌面实现统一认证。

9.5.2 易使用要求

应符合下列易使用要求：
a） 提供已预装、可下载安装应用软件的提示功能；
b） 提供P2V解决方案，迁移系统、应用和数据，原系统正常运行、数据一致。

9.5.3 一致性

虚拟桌面应用、远程应用及本地桌面应用间快捷方式的操作模式应保持一致。

9.5.4 部署/使用效率

应符合下列部署/使用效率要求：

a） 在正常运行的桌面云系统上添加/移除服务器设备的响应时间不宜超过3分钟；
b） 已安装部署的桌面云系统上，上传、发布常用应用的时间不宜超过3分钟；
c） 虚拟桌面重连耗时不宜超过3秒。

注：重连耗时为终端发起连接到虚拟桌面的时长。

9.5.5 资源管理

应支持通过链接、用户名、密码便捷接入各类受管云资源，以受管云平台、资源域等逻辑单位进行纳管。

9.5.6 告警管理

应符合下列告警管理要求：
a） 支持对告警事件按严重程度设定分级；
b） 支持对告警信息的统计分析。

9.5.7 智能分析

智能分析应符合下列要求：
a） 支持智能分析应用访问拓扑关系 ；
b） 支持智能分析应用访问性能；
c） 支持自动发现应用异常，帮助定位故障根因；
d） 支持闲置虚拟机识别，导出统计报告；
e） 支持智能发现虚拟桌面卡慢分析，并提供处置建议；
f） 支持虚拟桌面使用情况分析，包括桌面使用时长，软件使用情况及时长。

9.5.8 介质库管理

应符合下列介质库管理要求：
a） 提供软件文件的上传和管理；
b） 提供脚本文件的上传和管理；
c） 提供镜像文件的配置管理；
d） 提供配置文件的配置管理。

9.5.9 任务管理

应符合下列任务管理要求：
a） 支持配置运维命令或脚本；
b） 支持设置定时或周期性执行策略；
c） 支持云管平台巡检，包括云管平台组件的运行状态，以便发现问题和风险；
d） 支持云管平台配置数据的备份、恢复任务。

9.5.10 容量管理

应符合下列容量管理要求：
a） 支持对云资源总量、已使用量、可用量的整体统计；
b） 支持基于机房、集群等维度监控容量变化趋势，生成容量健康度提示。

9.5.11 大屏管理

应符合下列大屏管理要求：
a） 展示云管平台关键信息，如系统规模、资源分布、业务使用量统计排名等情况；
b） 展示云管平台的总体健康度、监控告警分布情况。

9.5.12 日志管理

应符合下列日志管理要求：
a） 支持记录所有角色的用户在系统进行的操作；

b） 支持每条操作日志应包含操作人、操作内容、操作类型、操作时间、操作结果等信息。

9.5.13 报表管理

应符合下列报表管理要求：

a） 支持查询权限内的资源实例信息、云基础资源平台信息等；
b） 提供一定程度的报表自定义功能，实现个性化的数据报表；
c） 支持报表导出为excel、CSV、PDF等至少一种格式；
d） 提供多维度统计报表，如集群维度、虚拟化类型维度、业务维度等；
e） 提供多种筛选条件，如时间段、物理或逻辑位置、服务类型、关键字等。

参 考 文 献

[1] GB/T 25069—2022 信息安全技术 术语
[2] GB/T 35292—2017 信息技术 开放虚拟化格式（OVF）规范
[3] GB/T 35293—2017 信息技术 云计算虚拟机管理通用要求
[4] GB/T 37950—2019 信息安全技术 桌面云安全技术要求
[5] T/CESA 9163—2020 信息技术应用创新 服务器虚拟化软件规范