



中华人民共和国通信行业标准

YD/T 2807.3-2015

云资源管理技术要求 第 3 部分：分平台

Technical requirements of cloud resource management
Part3: Sub-platform

2015-04-30 发布

2015-07-01 实施

中华人民共和国工业和信息化部 发布

目 录

前 言..... II

1 范围..... 1

2 规范性引用文件..... 1

3 术语和定义..... 1

4 缩略语..... 1

5 云资源管理平台的系统架构..... 2

6 分平台的技术要求..... 2

 6.1 分平台系统架构..... 2

 6.2 门户..... 3

 6.3 系统管理..... 3

 6.4 接口管理..... 3

 6.5 资源管理.....*

 6.6 设备管理..... 12

 6.7 监控管理..... 19

 6.8 日志管理..... 21

 6.9 统计分析..... 21

 6.10 安全管理..... 22

前 言

《云资源管理技术要求》分为五个部分：

- 第 1 部分：总体要求；
- 第 2 部分：综合管理平台；
- 第 3 部分：分平台；
- 第 4 部分：接口；
- 第 5 部分：存储系统。

本部分是《云资源管理技术要求》第 3 部分。

本部分按照 GB/T 1.1-2009 给出的规则起草。

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这些专利的责任。

本部分由中国通信标准化协会提出并归口。

本部分起草单位：中国联合网络通信集团有限公司、华为技术有限公司、工业和信息化部电信研究院、中国电信集团公司、中国科学院计算技术研究所。

本部分主要起草人：徐 雷、房秉毅、李素粉、陈 娜、陈 楠、王煜炜。

云资源管理技术要求

第 3 部分：分平台

1 范围

本部分规定了云资源管理的分平台的技术要求，包括分平台的系统架构，以及门户、系统管理、接口管理、资源管理、设备管理、监控管理、日志管理、统计分析、安全管理这些功能模块的要求。

本部分适用于基于基础设施即服务（IaaS）的云计算资源管理系统。

2 规范性引用文件

本文件对于下列文件的引用是必不可少的。凡是标注日期的引用文件，仅所注日期的版本适用于本文件。凡是不标注日期的引用文件，其最新版本（包括所有的修改版本）适用于本文件。

- YD/T 2807.1 云资源管理技术要求 第 1 部分：总体要求
- YD/T 2807.2 云资源管理技术要求 第 2 部分：综合管理平台
- YD/T 2807.4 云资源管理技术要求 第 4 部分：接口

3 术语和定义

下列术语和定义适用于本文件。

3.1

资源池 Resources Pool

一组物理资源或一组虚拟资源的集合，可以从池中获取资源，也可将资源回收池中。资源包括物理机、虚拟机、物理存储资源、虚拟存储资源、虚拟网络资源和物理网络资源等。

3.2

公网 IP Internet IP

云计算平台对外提供用于用户访问互联网的 IP 地址。

3.3

用户 User

云资源管理平台系统用户,包括运维管理用户和 IaaS 业务用户。

4 缩略语

下列缩略语适用于本文件。

FCSAN	Fibre Channel Storage Area Network	光纤直连的存储区域网络
FTP	File Transfer Protocol	文件传输协议
HTML	HyperText Markup language	超文本传输协议
IPSAN	IP Storage Area Network	基于 IP 技术的存储区域网络
JMS	Java Message Service	Java 消息服务
IO	Input/Output	输入/输出
NAS	Network Attached Storage	网络接入存储
P2V	Physical to Virtual	物理机到虚拟机

SLA	Service Level Agreement	服务等级协议
SAN	Storage Area Network	存储区域网络
SSH	Secure Shell	安全外壳协议
SCP	Security Copy Protocol	安全传输协议
SNMP	Simple Network Management Protocol	简单网络管理协议
SQL	Structured Query Language	结构化查询语言
Telnet	Telecommunications Network	远程登录协议
V2V	Virtual to Virtual	虚拟机到虚拟机
WebService		Web 服务
XML	Extensible Markup Language	可扩展标记语言

5 云资源管理平台的系统架构

云资源管理平台系统架构如图 1 所示，由综合管理平台和一個或多个资源管理平台（即分平台）组成。综合管理平台与分平台之间通过资源管理接口连接。云资源管理平台系统对客户提供服务，并为运维管理人员提供维护管理功能。

综合管理平台的内容请见 YD/T 2807.2 《云资源管理技术要求 第 2 部分：综合管理平台》。

综合管理平台和资源管理分平台之间的接口信息请见 YD/T 2807.4《云资源管理技术要求 第 4 部分：接口》。

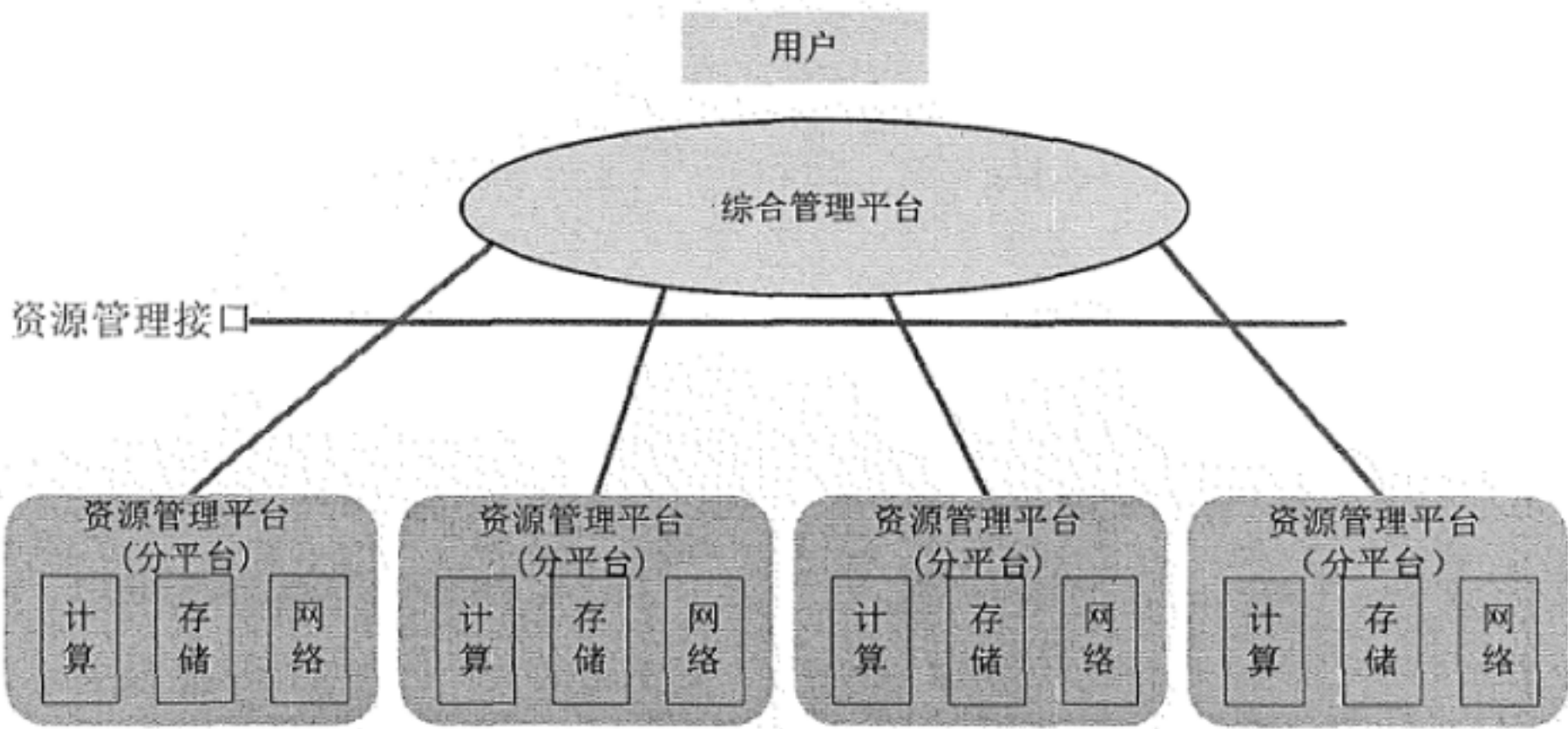


图1 云资源管理平台系统架构图

6 分平台的技术要求

6.1 分平台系统架构

分平台功能架构如图 2 所示。

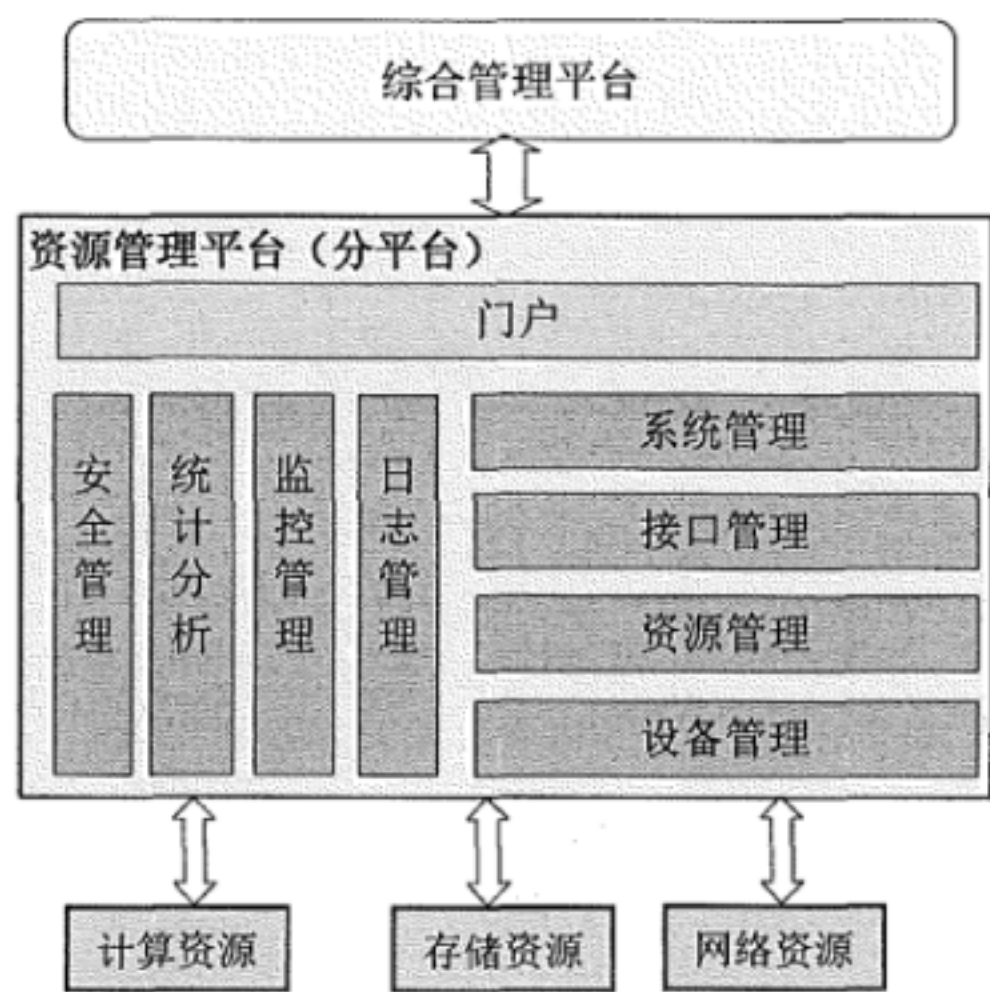


图2 分平台功能架构图

6.2 门户

门户为分平台的管理人员提供的操作界面和功能访问入口，管理员通过门户完成系统管理、资源管理、资源配置、设备管理、资源监控以及一些必要的运维管理的操作。

6.3 系统管理

6.3.1 用户管理

6.3.1.1.1 认证鉴权

应支持多种认证鉴权方式。

6.3.1.1.2 角色管理

提供用户角色管理：支持为用户赋予/取消角色；支持根据用户的不同角色制定多种用户界面，角色指权限的集合，可将不同权限添加到角色中，便于权限管理。

6.3.1.1.3 权限管理

权限管理模块能够对平台中的系统管理、资源管理、设备管理、资源的监控、服务实例等进行分级统一的权限分配和控制。支持管理员的增加、删除、信息修改、密码修改、查找等功能；支持将不同的管理权限划分给不同的管理员角色；支持为管理员分配、回收、更改管理员角色等功能。

6.3.1.1.4 用户与资源的绑定关系

不同用户拥有不同的资源操作权限，管理平台在配置用户的权限时，需要同时支持对操作权限的分配和用户与特定范围的资源的绑定，资源范围支持域级别的划分

6.4 接口管理

分平台需要和各种系统以及资源进行操作和数据的双向集成，以实现操作调度和返回结果。具体功能如下：

——资源调度应该支持尽可能多的设备和应用种类（包括各种操作系统、虚拟化、存储、网络），并可以通过开发增加支持的种类。

——针对设备与应用访问方式：建议对所有应用与设备的访问方式均采用无 Agent 方式，不在设备和应用上部署软件。调度平台与应用和设备交互均采用公开的业界标准协议（Telnet、SSH、FTP、SCP、SNMP、SQL、JMS、WebService 等协议），推荐加密通信方式如 SSH、SCP 等安全通信协议。

——针对外部访问与集成需要：资源调度采用标准化的外部接口方式，建议采用 Webservice，并使用加密方式确保访问与通信安全。

6.5 资源管理

6.5.1 概述

资源是指分平台所涉及到的各种物理设备和软件的集合，按其类型可分为服务器类资源（包括计算服务器等），存储类资源设备（包括 IPSAN、FCSAN 设备等），网络类资源（包括交换机和路由器等），虚拟机类资源（包括虚拟机模板等），软件类资源等。资源管理应提供对上述各类资源的抽象和信息记录，并对资源的生命周期、容量和访问操作进行综合管理。

6.5.2 计算资源

计算资源包括虚拟机资源、物理机资源。

分平台能够根据资源的类别进行分类，并列出具体的资源清单，主要包括物理服务器、虚拟机、网络设备、存储设备、IP 地址等资源的清单。当物理资源和虚拟资源发生变化时，分平台里面的资源清单能够根据变化实时动态更新。

分平台通过物理服务器配置系统对物理机资源进行部署和管理，为用户的物理机资源申请提供服务实例。为提高物理机资源池管理的灵活性，分平台应支持多种异构厂家服务器的配置系统。

分平台通过虚拟化软件对虚拟机资源进行部署和管理，为用户的虚拟机资源申请提供服务实例。为管理异构的虚拟机资源池，应该兼容多种虚拟化系统。

6.5.3 网络资源

网络资源是指虚拟化平台中使用的路由器、交换机、防火墙、负载均衡器、IP 地址和 VLAN 等。网络交换机和路由器在添加到分平台后，管理平台能够发现网络设备，并将其加入到管理平台，成为可被管理和调度的物理资源。可以由物理交换设备向分平台开放 API，实现分平台对物理设备进行管理。从而便于管理平台对网络的统一管理和控制，本项为可选，暂不做强制要求。

分平台可将网络资源整合为一个整体，对外提供统一的网络资源分配和集中式管理，如 IP 资源分配和负载均衡配置等。分平台应该提供集成和兼容不同网络设备的接口和能力。

6.5.4 存储资源

存储是指目前通用的块存储和文件存储等共享存储。存储在添加到分平台后，分平台能够发现存储，并将其加入到分平台，成为可被管理和调度的物理资源。

分平台通过存储设备管理软件实现对存储类资源的管理，将多个存储设备的资源整合在一起并抽象化，对外提供整体的出口和存储空间管理，让它看上去如同一个资源。

存储资源池可以由含有虚拟化能力的存储设备（如分布式文件系统、虚拟化存储）来承建。但分平台应该提供集成和兼容不同存储设备管理软件的接口和能力。

6.5.5 资源状况及生命周期管理

6.5.5.1.1 资源状况管理

资源状况管理对资源池的资源容量状况进行管理，可以对资源池中各类资源的资源总量、已分配资源、未分配资源进行统计，如果容量接近于饱和，会发出报警，提示管理员。

6.5.5.1.2 资源分配

分平台接收到资源申请指令，根据指令分配相应的资源，为分配的资源实例进行编号，记录资源实例相关的配置和描述信息。资源分配成功后，执行资源部署操作。

6.5.5.1.3 资源部署

资源部署操作通过设备管理接口在各类资源系统或设备上部署分配过的资源实例，部署成功后记录各资源实例的部署信息、配置信息、资源实例与资源系统或设备的关联关系等。

6.5.5.1.4 资源操作

分平台接收到资源操作指令，通过设备管理接口对指定资源实例进行操作。

6.5.5.1.5 资源回收

分平台接收到资源取消指令，通过设备管理接口对指定资源实例进行回收，回收成功后，将资源实例状态更改为已删除。

6.5.6 物理资源

6.5.6.1.1 资源管理

包括对物理服务器、存储服务器和网络设备等资源的管理。分平台支持根据预先配置，自动将设备纳入到平台进行管理。过程分为如下几个步骤：

- 为纳入管理的服务器分配 IP 地址；
- 自动安装指定操作系统；
- 自动安装虚拟化软件（包括计算虚拟化软件、存储虚拟化软件）和管理软件包。

6.5.6.1.2 资源清单

资源清单的获取支持通过静态配置或导入方式，分平台支持动态更新资源清单。

分平台提供在资源清单中进行资源快速定位的功能，主要包括：

支持在线查询：管理界面上支持直接输入待查询资源名称，如果有匹配资源，则直接转入到资源信息界面；

支持离线查询：支持管理员将资源信息导出到文件中，查询操作可以在导出结果中进行。

6.5.6.1.3 服务器管理

服务器管理是指针对各种操作系统实现服务器的完整生命周期的自动化管理。

- 资产信息和配置发现：系统能发现各种资产信息和配置信息，包括硬件、软件、操作系统等。
- 操作系统安装：支持虚拟机或物理机上安装多种操作系统，包括 Windows, Linux 等。同时，系统还支持直接从虚拟环境的模板以克隆的方式创建操作系统，并完成相应的定制操作。
- 补丁管理：系统支持针对 Windows, Linux 等操作系统的补丁管理功能，包括补丁分析、安装、检查和报表等。系统支持补丁自动化部署功能，包括：
 - 建立补丁介质库。
 - 用户在资源使用过程中，可以选择需要的补丁，进行自动化部署。在软件或补丁安装的过程中，如果出现问题，系统可以自动回滚到安装前的状态。
 - 提供补丁的安装和基线审核的自动化操作流程的增、删、改功能。
 - 提供补丁安装自动化操作流程执行过程中，安装参数输入、选择、临时性手工操作和安装信息反馈输出等功能。
 - 提供自动化的补丁分析功能，推荐需要安装的补丁。

——软件集中分发与安装：系统支持跨平台的软件统一存储，分发与分发后配置。系统可以分别定义作业的不同阶段(测试，下发介质，提交)的执行时间，同时可以对正在进行的作业强制中断，或对已经完成的变更作业进行回滚。

——日常巡检：系统支持对服务器进行日常健康检查，检查项目能够通过定义合规规则的方式进行定义，通过直观的表达逻辑组合即可完成检查设置，而无须进行大量的脚本编制工作。

——操作审计：通过系统对被管理的服务器进行的所有记录，系统均可自动记录并出具细节的操作报表。

——配置管理：系统支持对被管理服务器的关键配置进行定期快照，并在配置发生变化时自动产生告警。对于已发现的配置差异，可通过系统自动恢复到某个指定的快照配置。

——脚本执行：系统支持以集中的方式统一存储，分发和执行用户定义的指令和脚本，并可定期调度脚本的执行，统一收集脚本执行结果并出具相应的报表。

——报表：系统支持出具相应的运维报表，包括资产类报表，合规类报表，作业执行类报表，审计与操作记录类报表等。

6.5.6.1.4 网络设备管理

分平台能够实现对网络资源的统一调度和管理，主要包括：

——网络设备自动发现：分平台能够发现新添加的网络设备，并能获得网络设备的相关信息，主要包括设备型号、厂家信息、端口信息、网络带宽容量、VLAN 等。

——网络设备管理：分平台能够实现对网络设备的配置管理和资源监控，或通过调用第三方网管平台实现此功能。

——物理和虚拟机的网络属性：分平台能够对物理服务器和虚拟机占用的网络端口、网络流量、IP 地址、VLAN 等网络资源进行监控和管理。

——IP 地址管理：分平台能够提供网络 IP 的分发、配置、回收、统计等管理。

——网管接口：分平台能够对外提供网络资源池管理的操作接口。

——考虑到公网 IP 地址的有限性，网络设备管理需具备对公网 IP 进行管理，并提供 NAT 服务的能力。

6.5.6.1.5 存储管理

存储资源管理提供了对存储服务器基本信息记录和系统管理接口的封装，通过资源信息查询可以获取存储服务器信息并在上安装业务软件，监控模块通过其管理接口监视存储服务器的运行状态，部署调度模块可以将存储服务器作为弹性计算资源的载体并利用管理接口对其进行操作。

——配置：支持对指定存储服务器的配置，配置的内容包括：

- 服务器角色，例如计算服务器、存储服务器等；
- 待分配的 IP 地址；
- 待安装操作系统；
- 待安装存储虚拟化软件和管理软件包（例如，日志、监控等）。

——自动发现：分平台支持根据预先配置，自动将存储服务器纳入平台进行管理。具体步骤请参见资源纳管部分。补充资源纳管内容

——远程操作：分平台支持对存储服务器的远程上、下电和重启操作。

——状态监控：在将存储服务器纳入分平台后，分平台支持实时地从存储服务器中自动获取信息，包括服务器运行状态、管理软件运行状态和资源信息。资源信息具体包括：

- 服务器硬件信息，如 BI/OS 版本信息、单板编号等；
- 服务器 IP 地址；
- CPU 占用率；
- 内存占用率；
- 网络流入、流出；
- 虚拟存储资源分配统计；
- 业务进程状态统计。

6.5.6.1.6 网络拓扑

分平台能够实时显示物理服务器资源域、存储资源域、网络资源域、集群、数据中心的拓扑结构。当物理资源发生变化时，对应的资源域、集群的拓扑结构能够实时更新。

——自动发现：系统提供针对虚拟环境，存储和网络设备等基础设施的自动发现，拓扑关系绘制，查询等功能。其中，系统能够发现和解析物理网络设施和逻辑关系，以及应用的依赖关系。

——查询：系统提供对任何发现设备的查询能力，查询范围根据具体需要包括以下部分或所有参数：BI/OS，描述信息，DNS 名称，IP 地址，标签，位置，MAC 地址，制造商，型号，开放的 TCP 端口，操作系统类型，处理器速度，处理器/架构，软件补丁，软件产品，系统名称，以及对象类型。

——同步：通过直接的集成，自动发现可以自动将发现的数据结果同步到系统资源数据库中。

6.5.7 虚拟资源

6.5.7.1.1 资源池管理

资源池为租赁给最终用户的业务产品，资源池从服务的提供者和使用者的两个角度进行划分，包括提供者资源池和最终用户资源池，两者之间是一对多的对应关系：

——提供者资源池：由管理员创建并分配，支持不同的服务等级的资源池的创建与管理。

——最终用户资源池：最终用户负责向管理员申请后，在提供者资源池上创建，由最终用户独享并通过在资源池上创建虚拟机来提供服务。

——计算资源池：支持设置 CPU、内存资源的最低保留值、最大使用值和权重值。

——存储资源池：支持创建来自不同的存储资源的存储资源池。

——网络资源池：支持创建对内提供服务的网络资源池，网络资源池内的网络资源支持安全域的隔离，并能在网络资源池内实现 NAT、DHCP 等服务。

6.5.7.1.2 虚拟资源分配与调度（策略、流程）

通过自动执行操作流程以及跨系统管理职能的协调，提供资源部署的自动调度，能够根据管理员的设置，实现所需资源的自动选择、自动部署。替代容易出错的人为操作、加速系统之间的流转、大幅提升服务执行效率、并且提高结果的可靠性，更快、更好地完成任务。

资源调度的核心是调度引擎服务器，负责根据流程库中的脚本执行流程的调度，并且还应具备时钟控制、策略的执行、人机界面的交互等。

除了资源调度引擎之外，还需要有自动化部署模块，自动化部署模块实现资源端对端的安装和部署。

和其他的系统集成包括：由其他系统触发调度引擎、调度引擎调用其他系统的接口并传递相关参数、其他系统执行完任务后把结果反馈给调度引擎。

资源调度模块应该为所有接口提供抽象层，通过抽象层与被调度的应用双向交互，如果应用发生变化，只需要修改相应的抽象层，而无需对流程本身做任何修改。如创建虚拟机操作，通过抽象层用户无需关心创建虚拟机应用的具体平台和版本，甚至不需要了解创建虚拟机具体是什么应用完成的。抽象层将负责处理所有的细节，一旦创建虚拟机系统升级或变化，所有流程无需任何变化，只需要升级对应的抽象层即可。

——调度策略：调度策略模块提供资源部署的决策，搜集相关信息（资源使用情况、SLA 等），根据管理员的预定义的策略，自动选择服务实例所需的资源和启动对应的部署流程，同时允许管理人员手工干预部署。具体功能如下：

- 提供图形化的设计界面，来制定策略判断规则。
- 可以通过集成接口从其他系统中获取相关的信息，自动决策判断。也可以综合各方面的信息，集中展现，作为人工判断的依据。
- 允许在判断的步骤中设置人工的控制点，补充信息、中断操作等。
- 在策略判断中可以根据不同的判断条件来计算，实现各种逻辑操作及其灵活组合。

——资源调度：调度引擎是业务流程管理的运行和控制中心，它负责把任务分派给执行者，并根据任务执行的返回结果决定下一步的任务，控制并协调各种复杂工作流程的执行并且同步各个客户端的反应。具体功能如下：

- 子流程嵌套使用：子流程对应着实例级的策略。流程之间可以相互调用，把其他的流程作为主流程的一个环节，这包括可重用性，继承和抽象。可以通过授权为不同资源管理人员配置各自的子流程（例如部署虚拟机的子流程），然后在向用户提供计算服务的主流程中直接调用一个或多个预定的子流程协调完成相关的任务。实现统一调度引擎平台下，多系统的协调合作。

- 必要时的回退：为保障流程执行操作的完整性，必要时设置退回机制，这方面需要业务的类型和被管对象的支持。

- 流程路径：流程的流转支持（并行、串行、混合）等各种灵活的方式。
- 工干预：允许管理员在必要的时候人为介入流程，补充某些信息、起停相关的步骤等控制操作。
- 流程的权限控制：流程的模板应该按照惯例的业务、部门、人员权限等进行安全隔离的存储，只有经过授权的人员才可以查看、使用。

- 流程配置的导入和导出：通过标准的方式（例如 XML）可以实现流程配置信息的导入和导出。

——调度流程执行：提供对流程的管理与监控功能，包括对已部署的业务流程的管理功能（启用、禁用、舍弃等），以及流程的流转跟踪等。具体功能如下：

- 流程的触发：1、能够自动接收和探测不同的事件，进而根据预定规则执行相应的流程；2、在内置向导的引导下分步骤由管理员来启动并参与完成，根据用户需要选择全自动或半自动模式；3、基于某个时间段或频率来进行调度输入。

- 输入：通过标准的接口输入相关的流程信息。
- 流程执行的判断：在流程执行中可以根据不同的判断条件来执行不同的操作，实现各种逻辑操作及其灵活组合。

- 参数的传递：采用标准的方式，建议使用 XML 作为统一的交互方式资源调度数据，组件间通信均采用加密方式（例如 HTTPS），所有内部通讯均不可伪造与篡改。

- 监控点：对调度引擎的运转可以设置监控点，必要时由管理员人工进行干预。同时根据系统命令结果执行自动告警，告警方式可根据需要灵活调整，实现包括 SNMPTrap、邮件和告警平台联动在内多种告警方式。

- 输出：调度引擎通过标准的接口，向其他系统发送调用命令和相关的参数。

- 故障接管：资源调度系统的稳定可靠对环境的运行至关重要，必须提供高可靠性的保障机制，任意节点失效都可被其他节点自动接管。保障系统不但能够克服任意单个故障，甚至多个节点故障都不会影响其流程的正常执行。

——集成接口：资源调度系统需要和各种系统以及资源进行操作和数据的双向集成，以实现操作调度和返回结果。具体功能如下：

- 资源调度应该支持尽可能多的设备和应用种类（包括各种操作系统、虚拟化、存储、网络、数据库、中间件和应用软件），并可以通过开发增加支持的种类。

- 针对外部访问与集成需要：资源调度采用标准化的外部接口方式，建议采用 Webservice，并使用加密方式确保访问与通信安全。

——自动部署：自动部署管理实现对网络、存储、操作系统、补丁、数据库、中间件、Web 服务器、应用程序等进行集中部署、更改、回收的功能。

——网络资源部署：通过网络配置部署平台可实现复杂多供应商网络基础环境中的自动配置和管理，实现端到端的自动化。能控制和检查整个网络基础结构中的配置变更，集中定义、核查、强制执行网络安全政策以及配置规范相关的合规性。网络配置管理自动化包括设网络各初始配置，打补丁，配置变更，配置规则强制执行，安全漏洞修复等。

——计算资源统一部署：计算资源统一部署支持对各种操作系统和虚拟化计算资源进行集中控制、批量自动化安装，结合设备厂商提供的部署工具，计算资源统一部署可以控制服务器的引导过程。允许用户预定义安装服务器所需要的配置模板，比如：IP 地址、主机名、管理员口令、磁盘分区、安全设置、操作系统部件等，在模板中可以引入变量以增加模板的通用性。计算资源统一部署模块根据配置模板生成安装操作系统的自动应答文件，从而集中控制操作系统的部署和修复。

——存储部署：通过存储配置部署平台可实现复杂多供应商存储环境中的自动配置和管理，实现端到端的自动化。根据设备的管理方式采用直接对设备的配置操作或者集成存储厂商的设备管理工具，实现对存储的统一配置管理。

——补丁分发：软件管理模块可以联机或脱机方式获取各厂家最新的补丁信息，从而对系统当前的补丁进行分析，推荐应该安装的补丁。在导入补丁之后，软件管理模块可以根据补丁的平台自动生成补丁安装指令。如果在安装补丁前后需要执行一些操作（比如启停应用或服务），软件管理模块允许用户定义这些操作。软件管理模块支持在一次补丁安装过程中安装多个补丁或者补丁的 bundle，安装的对象可以为一组服务器。

——软件部署：可以分发的软件包括数据库、中间件、Web 服务器、用户自开发应用等。在导入软件介质之后，软件管理模块可以根据介质的平台自动生成安装指令。跟软件安装相关的操作可以捆绑成一个独立的安装包，安装包中可以包括各种安装要素，如应用或补丁的安装介质、脚本、配置文件、配

置参数、目录、服务、用户、组、注册表、安全设置等。在安装包中还可以设定在单用户模式或正常模式下安装、安装顺序、是否需要重启、卸载命令、文件权限、服务的状态等。软件管理模块可以在一个安装包中部署分布式应用到多台不同的服务器上，比如部署 J2EE 等多层架构应用。

——资源回收：根据管理策略利用资源调度引擎对服务到期、服务中止、欠费客户的计算资源和网络资源进行回收，包括关闭虚拟机或物理器，回收 VPN 使用 IP、公网 IP、虚拟交换机，取消与之相关的存储资源、负载均衡设备、交换机等相关配置，并更新资源库的信息，具体回收的操作需要集成设备的管理能力。

——资源分配：计算资源，包括计算资源（CPU、内存）、存储资源和网络资源，在资源部署调度中，应能够针对三种资源进行管理和维护，主要包括：

- 资源的统计和使用分析能够统计在一个虚拟化环境中所有的资源数量以及资源使用情况，资源的统计主要包括 CPU 总数、内存总数、存储总数以及可用网络总数等。资源使用情况分析主要包括总的 CPU、内存使用情况、网络流量分析、存储使用情况、存储吞吐量分析等。

- 资源的分组（资源域）能够按照域的概念将资源分为不同的组，可以按照资源类型来分，也可以按照业务种类来分。

- 资源部署调度应该能够从资源池中自动获取相应的资源来组成新的虚拟机，或者调整虚拟机的资源分配，从虚拟机中释放掉的资源，应能够自动返还给资源池，资源分配模块还应该具备资源应用报表统计的功能，从而帮助管理员更好的管理资源。

——资源动态增减：虚拟机所占用的资源能够进行动态的增减，在动态增减是，不会导致虚拟机对外的服务终端。用户可以自定义动态增减的规则，这些规则主要包括资源动态增减的阈值设置和最小的资源占用、最大的资源占用，以及虚拟机的资源动态调配优先级。当一个虚拟机的负载的增大时，如果超出制定的阈值，根据事先制订的资源分配规则，并判断该虚拟机的优先级，当确定符合要求后，则分配增加的资源给该虚拟机。如果该虚拟机所在的物理机不能提供相应的资源，系统会自动将该虚拟机迁移到其他能够满足资源需求的物理机上。或者将资源优先级更低虚拟机迁移到其他物理机上，从而获得资源追加给该虚拟机。资源的动态增减支持自动模式，同时也应该支持手动模式，直接手动调整虚拟机的资源占用。资源的动态增减应包括 CPU 和内存的增减调整。

——资源绑定：能够将某虚拟机所使用的资源同物理实际资源进行一对一的绑定，或者可以解释为资源的独占。资源的绑定至少要支持一下几种资源：

- CPU 绑定：能够指定虚拟机的虚拟 CPU 独占一个 CPU 核，从而得到稳定的计算能力。
- 内存的绑定：能够指定虚拟机的虚拟内存独享一定大小的物理内存，保证该部分内存不会出现 SWAP 性能降级的情况。
- 网卡的绑定：能够指定虚拟机的网卡同物理机的网卡实现独占方式。从而保证虚拟机的网络带宽。
- 当虚拟机进行迁移时，资源部署调度会尽可能的去申请能够满足资源绑定需求的物理机位置进行迁移，当没有可以满足的物理机是，可以设定迁移后的资源绑定策略，这些策略应包括：
 - 强制迁移：不管迁移的目的物理机是否有相应的资源用来提供绑定，都进行迁移，迁移后会生成警告信息通知管理员
 - 中断迁移：迁移时会中断而导致迁移失败，系统生成警告信息通知管理员，并且根据管理员的指定确定是否继续强制迁移。

——资源使用优先级：资源使用优先级是实现分平台量化管理和集中控制的重要机制，要求所有优先级的指标必须可以灵活配置，可以灵活设置控制点和相关管理阈值。

——资源优先级：可以将不同的物理资源进行分类管理，可以设置为金牌、银牌资源、铜牌资源的类别，针对不同的用户级别，可靠性的要求，智能的对物理资源进行分配。通过这个功能，能够在一个域中优先使用性能较好的资源。

——虚拟机资源优先级：虚拟服务器设置对资源的占用优先级，至少应支持高、中、低三个级别，当多个虚拟服务器共享 CPU、内存和 I/O 等资源并且虚拟机发生动态资源增减、动态迁移等动作时，优先级高的虚拟机会优先抢占空闲的资源。当总资源需求不满足时，优先级低的虚拟机将被强制释放掉一部分资源来保证优先级高的虚拟机使用。释放后的最低值受到动态资源增减中下限资源占用的限制。

——用户使用资源优先级：可以定义用户的服务级别，用户的等级不同，在资源分配、使用上进行分级管理，根据用户对资源的需求程度，应支持多个级别的用户分类。

——迁移：分为以下几种：

- 虚拟机迁移：虚拟机由安装在一台物理服务器上，转移到另外一台物理服务器上之后，在迁移的过程中仍然能够正常运行并继续提供服务，要求在迁移的过程中有较好的数据传输策略来达到较低的网络带宽占用。

- 存储迁移：虚拟机的存储数据由一台存储设备迁移到另一台存储设备，迁移前后虚拟机的运行状态保持连续性和一致性。存储的迁移过程中应不会导致虚拟机的业务中断。

- 迁移是指虚拟服务器的位置，由安装在一台物理服务器的虚拟机管理程序（Hypervisor）上，转移到另外一台物理服务器的虚拟机管理程序（Hypervisor）上之后，仍然能够正常运行并继续提供服务。在这一过程中一般不需要对服务器设置进行任何更改。当物理服务器设备需要维护，或者在为了减少耗电需要关闭部分物理服务器时，可以利用虚拟服务器迁移技术。虚拟服务器的迁移功能表现了服务器虚拟化对资源的抽象化和计算资源相对物理设备的独立性。

- 虚拟服务器需支持离线迁移和在线迁移两种不同的迁移形式：离线迁移：虚拟服务器停止运行后，通过共享存储或者存储复制等方式，迁移到另外一台物理服务器上重新启动。在相同类型或兼容的虚拟机管理程序（Hypervisor）支持下，两台物理服务器配置不同、存储方式不同的时候，仍然可以进行离线迁移。在线迁移：如果两台物理服务器使用同类 CPU、不绑定特定硬件，并采用网络共享存储，能够支持在业务不中断的情况下，实现虚拟服务器从一台物理服务器迁移到另一台物理服务器，即在线迁移。

——负载均衡：当某一物理机的总资源占用达到预先设置的阈值是，系统会自动将该物理服务器上的某台虚拟机迁移到其他物理机上，从而保证动态的负载均衡；资源部署调度功能实体持续监测集群内所有主机和虚拟机的 CPU 和内存资源的分布情况和使用情况。在给出集群内资源池和虚拟机的属性、当前需求以及不平衡目标的情况下，会将这些衡量指标与理想状态下的资源利用率进行比较。然后执行相应地虚拟机迁移（或提供迁移建议）。

——节能管理：当单台物理机的资源占用小于预先设置的阈值时，系统应能够支持 CPU 的自动降频技术，自动降低 CPU 主频从而达到节电目的。当大于某一阈值时，又能自动恢复 CPU 频率。当物理机平均资源占用小于预先设置的阈值时，能够将某台物理服务器的所有虚拟机迁移到其他服务器上，并且关闭该物理机电源，以减少设备耗电，当物理机平均负载上升到某一阈值时，能够重新打开被关闭的物

理机电源并启动物理机，当该物理机的资源加入到资源池时，系统又会将其他高负载服务器上的部分虚拟机迁移到该服务器上。

——资源调度策略：虚拟服务器自身的资源调度，或者虚拟服务器在不同物理服务器之间的迁移可以由管理员手动进行，也可以按照事先设置的策略自动进行。通过策略可以实现虚拟服务器资源配置的自动化和智能化，提高设备资源利用率和系统可用性。资源调度策略的触发方式包括：

- 定时：在预先设定的时间触发资源调度或迁移。
- 资源利用率阈值：当虚拟服务器的资源利用率达到预先设定的阈值时，触发对资源的重新配置或者虚拟服务器在线迁移。
- 应用运行状况阈值：当虚拟机中的应用程序触发到预先设定的阈值时，触发对资源的重新配置或者虚拟服务器在线迁移。
- 在触发自动迁移过程时，系统能够自动发现满足资源需求的物理服务器，并根据预先设定的策略自动选择合适的目标物理服务器完成迁移。

6.6 设备管理

6.6.1 虚拟机管理

6.6.1.1.1 概述

虚拟机管理提供对基于不同虚拟化系统的虚拟机的统一管理，指厂商提供给用户的虚拟化管理界面的可操作性，包括虚拟机生命周期管理、资源分配、批量部署、物理机向虚拟机的迁移、其他虚拟机向虚拟机的迁移、复制、迁移、快照和调度等等。

——虚拟机生命周期管理：

虚拟化管理界面可以实现虚拟机的创建、资源分配、运行控制、删除和资源回收等操作。

对于每台虚拟机可以通过模板设置资源或者手工分配修改资源，如 CPU 的数量、内存的大小、网卡的数量等。

管理员可以在管理界面上方便的选择启动、关闭、重启虚拟机并在界面上有相应的运行状态提示。

——虚拟机配置：

包括对虚拟机和虚拟卷的配置。

虚拟机的配置包括对虚拟机虚拟 CPU 个数、内存大小、系统卷容量、网卡数量、镜像类型等信息的配置。

虚拟卷的配置包括对用户卷容量、与虚拟机的绑定关系等信息的配置。

——虚拟机批量部署：

可以通过模板快速批量部署虚拟机，管理员可以根据需求安装配置一台虚拟机，做好相应的系统配置，然后通过复制功能将该虚拟机快速复制多份。复制的时候可以选择复制出来的虚拟机的硬件资源（CPU、内存），复制的数量，存储的类型，并自动分配虚拟机名称。所复制出来的虚拟机在应用和配置上和原有虚拟机完全相同。

——P2V 转换：

可以离线或者在线的将物理服务器上的操作系统（Windows/Linux 等）转换到虚拟环境。转换之前可以设置好虚拟机的硬件资源，被转换的操作系统在转换结束之前应该能自动检测并替换原有的硬件驱动以保证转换结束后能够在虚拟环境下正常启动。

——V2V 转换:

支持将其他主流虚拟化的虚拟机转换到自己的虚拟化环境,可以自动检测并替换原有的虚拟硬件设备以保证虚拟机在转换后的正常运行。

应该具有图形操作界面方便管理员操作,整个操作过程要求简便易行。

——虚拟机克隆:

支持可通过克隆现有虚拟服务器的方式快速创建虚拟服务器。

克隆不应影响被克隆的虚拟服务器。

除必要的参数配置以外,克隆过程可以自动化进行。

——虚拟机快照:

支持对虚拟机进行快照操作。

并且对运行状态的虚拟机的性能不会造成严重影响。

同时提供快照的越级恢复能力,即随意挑选不同时间的快照进行正确恢复。

——虚拟机运行控制:

可以在管理界面选择虚拟机的启动、关闭、暂停、重新启动等操作并在管理界面上有虚拟机相应的状态描述。

6.6.1.1.2 虚拟机创建

资源管理接受虚拟机创建请求,构造虚拟机编号并选择计算资源,将虚拟机的创建指令发送给虚拟机管理,指令中携带虚拟机基本信息和位置信息等,虚拟机管理返回响应。资源池管理下发配置虚拟机网络的指令到网络管理,携带网络的信息和虚拟机信息。

流程描述:

- 资源池管理收到虚拟机创建请求;
- 资源池管理返回虚拟机创建响应,响应中携带创建虚拟机编号;
- 资源池管理选择计算资源;
- 资源池管理向虚拟机系统发送虚拟机创建指令,携带计算虚拟机信息和位置信息;
- 虚拟机管理根据指令中的虚拟机信息和位置信息,将虚拟机创建至指定物理机;
- 虚拟机管理向资源池管理返回操作结果;
- 资源池管理向网络管理发送网络配置指令;
- 网络管理根据指令配置虚拟机的网络;
- 网络管理返回操作结果。

6.6.1.1.3 虚拟机操作

资源管理接受虚拟机操作请求,资源池管理根据操作请求类型对虚拟机执行启动、睡眠、停止、恢复、重启操作,并返回最终的操作结果。

流程描述:

- 资源池管理收到虚拟机操作请求;
- 资源池管理向虚拟机系统发送虚拟机操作指令;
- 虚拟机管理对虚拟机进行启动、休眠、停止、恢复、重启操作;
- 虚拟机管理向资源池管理返回操作结果;

——资源池管理返回虚拟机操作响应。

6.6.1.1.4 虚拟机查询

资源管理接受虚拟机查询请求，资源池管理根据操作请求获取虚拟机信息，并返回最终的查询结果。

流程描述：

- 资源池管理收到虚拟机查询请求；
- 资源池管理向虚拟机管理发送虚拟机信息查询指令；
- 虚拟机管理获取虚拟机信息；
- 虚拟机管理返回虚拟机查询结果；
- 资源池管理返回虚拟机查询响应。

6.6.1.1.5 虚拟机规格更改

资源管理接受虚拟机配置更改请求，资源池管理根据操作请求获取虚拟机配置信息更改信息，修改虚拟机的配置信息。

流程描述：

- 资源池管理收到虚拟机规格更改请求；
- 资源池管理向虚拟机管理发送虚拟机规格更改指令；
- 虚拟机管理更改虚拟机规格；
- 虚拟机管理返回虚拟机规格更改结果；
- 资源池管理返回虚拟机规格更改响应。

6.6.1.1.6 虚拟机访问

对于绑定公网 IP 地址的虚拟机，用户可通过远程控制协议（例如 RDP、SSH 等）使用客户端软件直接进行远程控制操作。

6.6.1.1.7 虚拟机备份

资源管理接受虚拟机备份的请求，资源池管理根据操作请求获取虚拟机信息，资源池管理首先将请求中指定的虚拟机制作备份，然后资源池管理将该虚拟机的备份保存至存储空间中。

流程描述：

- 资源池管理收到虚拟机备份请求；
- 资源池管理向虚拟机管理发送创建虚拟机备份指令；
- 虚拟机管理对虚拟机进行备份操作，备份数据保存到临时空间；
- 虚拟机管理返回创建虚拟机备份结果；
- 资源池管理向存储管理发送保存虚拟机备份指令；
- 存储管理保存虚拟机备份数据；
- 存储管理返回虚拟机备份结果。

6.6.1.1.8 虚拟机备份恢复

资源管理接受虚拟机备份恢复的请求，资源池管理根据操作请求获取虚拟机备份和虚拟机的信息，虚拟机备份恢复相应的虚拟机，并返回操作结果。

流程描述：

- 资源池管理收到恢复虚拟机备份请求；

- 资源池管理向存储管理发送获取虚拟机备份信息指令；
- 存储管理获取虚拟机备份信息；
- 存储管理返回获取的虚拟机备份响应；
- 资源池管理向虚拟机系统发送恢复虚拟机备份指令；
- 虚拟机管理执行恢复虚拟机备份操作；
- 虚拟机管理向资源池管理返回恢复虚拟机备份响应。

6.6.1.1.9 虚拟机删除

资源池管理接受虚拟机删除的请求，资源池管理根据请求删除指定虚拟机，并释放相关系统资源，所释放系统资源可以回收到资源池。

流程描述：

- 资源池管理收到虚拟机删除请求；
- 资源池管理向虚拟机管理发送虚拟机删除指令；
- 虚拟机管理终止虚拟机并释放相关的资源；
- 虚拟机管理向资源池管理返回结果；
- 资源池管理向网络管理发送释放网络配置指令；
- 网络设备根据指令删除相关的网络配置；
- 网络设备向资源池管理返回结果；
- 资源池管理释放虚拟机相关资源；
- 资源池管理返回虚拟机删除响应。

6.6.2 模板和镜像管理

6.6.2.1.1 模板管理

分平台需要具备虚拟机模板管理和服务模板管理的功能，提供虚拟机自动生成、自动部署功能，在业务需要海量服务节点的时候，能够以简单、高效的方式批量部署虚拟机，提高虚拟机生成效率，减少业务环境准备时间，更好的支撑业务服务。

分平台应提供预置的模板，也支持管理员自定义所需的模板。模板应既能支持各种操作系统，又能支持系统软件或应用软件，具体内容包括：

- 虚拟机的配置，如 CPU、内存、硬盘；
- 虚拟机的操作系统环境，如操作系统类型、版本；
- 虚拟机的应用软件环境，如软件安装包路径、安装参数；
- 应用软件的部署与配置流程，用于生成虚拟机时软件的安装与设置。

模板管理需要提供对主流虚拟化技术的模板管理功能，对已支持模板管理功能的虚拟化系统，分平台通过虚拟化系统提供的 API 接口，集成其模板管理功能。对于不支持模板管理功能的虚拟化系统，分平台需自己提供相应的功能。模板管理的具体功能如下：

- 提供模板的创建向导；
- 支持模板的修改、删除等操作；
- 支持模板的发布与撤销操作；
- 支持模板的权限管理，可指定能使用该模板的用户；

——提供预置的虚拟机模板，同时支持用户自定义虚拟机模板。

6.6.2.1.2 镜像管理

虚拟化管理平台能够实现虚拟机镜像文件的导入、导出功能，支持 OVF 标准格式镜像文件的导入和导出，支持针对镜像文件的快照功能。

6.6.2.1.3 模板的部署与部署后定制

系统支持通过用户通过门户申请基于模板的虚拟机实例，系统自动根据服务目录与虚拟机模板的映射关系创建虚拟机，并完成相应的操作系统定制，包括主机名，用户名，密码，网络设定，存储，以及用户选定的软件包，补丁的部署作业。

6.6.3 物理机管理

6.6.3.1.1 物理机申请

资源管理接受物理机申请请求，生成物理机标识，选择物理机资源，将申请物理机资源请求发送给物理机管理，指令中携带物理机基本信息和位置信息等，物理机管理返回响应。

6.6.3.1.2 物理机操作

资源管理接受物理机操作请求，资源池管理根据操作请求类型对物理机执行启动、睡眠、停止、恢复、重启操作，并返回最终的操作结果。

6.6.3.1.3 物理机查询

资源管理接受物理机查询请求，资源池管理根据操作请求获取物理机信息，并返回最终的查询结果。

6.6.3.1.4 物理机访问

对于绑定公网 IP 地址的物理机，用户可通过远程控制协议（例如 RDP、SSH 等）使用客户端软件直接进行远程控制操作。

对于具有私网 IP 地址的物理机，用户可以通过管理平台，在 web 浏览器中远程访问物理机。

6.6.3.1.5 物理机释放

资源管理接受物理机释放的请求，资源池管理根据请求释放指定物理机资源。

6.6.4 块存储管理

6.6.4.1.1 创建块设备

资源池管理接收到创建块设备请求后，选择块存储资源，向设备管理中的块存储管理发送创建块设备指令，指令中携带块设备信息，包括容量信息、位置信息等。块存储管理执行请求，分配并创建块设备，并返回响应，响应中携带分配的块设备标识。

流程描述如下：

——资源池管理接收到创建块存储请求；

——资源池管理选择块存储资源；

——资源池管理向指定块存储资源发送创建块设备请求，请求中携带块存储设备信息，包括容量信息、位置信息等；

——块存储管理执行创建块存储操作；

——块存储管理向资源池管理返回创建块存储响应，响应中携带块存储设备标识；

——资源池管理返回创建块存储响应，响应中携带块存储设备标识。

6.6.4.1.2 挂载块设备

资源池管理接收到挂载块设备请求后，根据虚拟机标识和块设备标识，由虚拟机管理指定虚拟机所在虚拟机管理程序（Hypervisor）与块设备所属块存储资源之间建立连接，把块设备挂载给相应的虚拟机。

流程描述如下：

- 资源池管理接收到挂载块设备请求，请求中携带虚拟机标识、块设备标识；
- 资源池管理获取相关的虚拟机资源信息、块存储资源信息；
- 资源池管理向指定虚拟机管理发送挂载块设备请求；
- 虚拟机管理所在虚拟机管理程序（Hypervisor）发起块存储连接请求；
- 块存储管理执行建立连接操作；
- 块存储管理返回连接响应；
- 虚拟机管理接收到响应后，挂载块设备至指定虚拟机；
- 虚拟机管理返回挂载块设备响应；
- 资源池管理返回挂载块存储的响应。

6.6.4.1.3 卸载块设备

资源池管理接收到卸载块设备请求后，由虚拟机管理指定虚拟机所在 Hypervisor 释放与块设备所属块存储资源之间的连接，从相应的虚拟机卸载块设备。

流程描述如下：

- 资源池管理接收到卸载块设备请求，请求中携带虚拟机标识、块设备标识；
- 资源池管理向指定虚拟机管理发送卸载块设备请求；
- 虚拟机管理从指定虚拟机上卸载块设备；
- 虚拟机管理指定虚拟机所在虚拟机管理程序（Hypervisor）发起释放块存储连接请求；
- 块存储管理释放连接；
- 块存储管理返回释放响应；
- 虚拟机管理返回卸载块设备响应；
- 资源池管理返回卸载块存储的响应。

6.6.4.1.4 删除块设备

资源池管理接收到请求后，向块存储管理发送删除块设备操作请求，块存储管理释放块设备。待删除的块设备应该处于未挂载状态。

流程描述如下：

- 资源池管理接收到删除块设备请求，请求中携带块设备标识；
- 资源池管理选择块存储资源；
- 资源池管理向指定块存储资源发送删除块设备请求，请求中携带块设备标识；
- 块存储管理执行删除块设备操作；
- 块存储管理向资源池管理返回删除块设备响应；
- 资源池管理返回删除块设备响应。

6.6.4.1.5 查询块设备

资源池管理接收到请求后，向块存储管理发送查询块设备信息请求，块存储管理获取并返回块设备信息，包括容量、状态等。

流程描述如下：

- 资源池管理接收到查询块设备请求，请求中携带块设备标识；
- 资源池管理选择块存储资源；
- 资源池管理向指定块存储资源发送查询块设备请求，请求中携带块设备标识；
- 块存储管理获取块设备信息，包括块设备容量、状态等；
- 块存储管理向资源池管理返回查询块设备响应，携带块设备容量、状态等；
- 资源池管理返回查询块设备响应，携带块设备容量、状态等。

6.6.5 网络管理

6.6.5.1.1 概述

资源池网络管理是将多个网络资源整合为一个整体，对外提供统一的网络资源分配和集中式管理。资源池网络管理应包含下面信息：资源池网络管理编号、网络资源类型、资源池网络管理组成信息、资源池网络管理容量信息、资源池操作方式、资源池访问接口等，资源池内应包括 IP 地址、VLAN、路由器、交换机、防火墙、负载均衡设备等，设备的形态可以是物理的，也可以是虚拟的。对于计算和存储资源虚拟化程度较高的数据中心，建议引入网络虚拟化技术，对网络设备进行虚拟化，实现网络资源云化。

6.6.5.1.2 网络资源池调度和管理

资源池网络管理能够实现对网络资源的统一调度和管理，通过对资源池网络管理的创建，修改，查询和删除，为综合管理平台提供自动化的网络供应接口。

提供对池类资源的生命周期管理（包括虚拟机的网络地址分配、回收等）。

在池类资源的整个生命周期内，提供状态监控，回收告警、自动回收等。

提供对池类资源的操作和管理接口。

能够单独或者批量增加资源池设备。

资源池网络管理平台能够对物理服务器和虚拟机占用的网络端口、网络流量、IP 地址、VLAN 等网络资源进行监控和管理。

IP 地址管理-资源池网络管理平台能够提供网络 IP 的分发、配置、回收、统计等管理。

网管接口-资源池网络管理平台能够对外提供资源池网络管理的操作接口。

支持虚拟机迁移且不中断业务，支持虚拟机远距离动态迁移技术。

核心设备具备集群的技术能力，以支持 IT 资源共享环境下的分级需求。

核心网络与接入网络互连时能够实现跨交换机的端口捆绑，提高冗余能力和链路互连带宽的同时，大大简化网络维护，以支撑虚拟化环境下的业务分流网络资源查询和定位（能通过请求规格，返回满足要求的资源信息）。

6.6.5.1.3 虚拟机的网络管理

在虚拟化环境中，虚拟机网络交换尤其重要，需要通过网络的虚拟化技术做到虚拟机的网络感知，在此感知的基础上，实现虚拟机流量的识别和控制，有如下功能：

——虚拟机的网络属性应包括：VLAN、QoS、ACL、带宽等。

——虚拟机的网络属性可以跟随虚拟机的迁移而动态迁移，不需要人工的干预或静态配置，从而在虚拟机扩展和迁移过程中，保障业务的持续性。

- 虚拟机迁移时，与虚拟机相关的资源配置，如存储，网络配置随之迁移，迁移过程业务不中断。
- 同一物理机或者不同物理机上的虚拟机之间的负载均衡。
- 虚拟网络本身要支持 HA。

6.6.5.1.4 网络安全管理

——资源池外部安全：安全设备应支持并使用如下的安全技术手段：

- 支持对互联网木马僵尸网络的报警与阻断功能；
- 支持 TCP 头检测，扫描与 DoS 检测；
- 支持对定制主机的定时阻断；
- 支持单个源 IP 的链接数限制；
- 支持动态策略生成与取消机制；
- 支持深层协议检测防御攻击。

——资源池内部的安全：数据中心内部不同区域间的安全主要依靠防火墙的安全域来实现，根据业务需求定义多个逻辑防火墙，多个逻辑墙共享物理防火墙的硬件，但彼此独立工作，每台逻辑墙均可完成物理防火墙的所有安全功能。在实现安全域时应遵循如下原则：

- 业务相关性原则；
- 高可用性原则；
- 资源分配原则；
- 安全策略最大化原则；
- 分权分级管理原则。

——资源池内部虚拟机之间的安全：

• 虚拟机之间的安全主要依靠虚拟防火墙来实现，虚拟防火墙本身可以 HA。可以创建 zone, 包含不同安全等级的区域，包含但不限于以上区域。

- 在防火墙上创建策略。
- 虚拟防火墙提供安全组功能，确保不同租户的虚拟机之间的网络隔离（包括同一个物理主机内的不同虚拟机）。针对每个安全组可以定义 ACL 规则，如对外开放某个具体的服务或端口，允许外部某个 IP 地址访问虚拟机的某个端口，也可安全组之间相互授权访问。

- 资源池网络管理要能防止同一个物理主机内虚拟机嗅探到其它虚拟机的数据包。
- 资源池网络管理要有能力防止恶意虚拟机的 IP 欺骗和 ARP 地址欺骗，限制虚拟机只能发送本机地址的报文。

6.6.5.1.5 QoS 管理

QoS 管理主要涉及业务分类、标记、调度管理、限速等。对于资源池网络管理平台。虚拟机的 QoS 管理。

识别虚拟机流量并根据业务类型打上相应的 CoS 标记。

能够根据不同虚拟进行不同粒度的限速。

提供调度能力以保证不同业务的服务质量（QoS）。

支持单虚拟机的网络流量控制以保证在大网络流量时不影响其他虚拟机的网络带宽。

6.7 监控管理

6.7.1 网络监控

网络监控包括：

——配置管理：提供对于网络设备的配置管理，包括带宽配置、VLAN 配置、NAT 转换配置、防火墙策略配置等功能；

——监控管理：支持对于路由器、交换机、防火墙、NAT 等网络设备的监控管理，监控的内容主要包括运行状态、端口流量等信息。

资源池系统管理员具有管理整个资源池中的网络设备的权限，普通管理员具有部分权限。

6.7.2 资源监控

资源监控用于管理员对资源管理分平台中的各类资源、设备进行监控，提供对各类资源、设备的性能监控、故障报警、能耗管理等功能。

可监控资源池中 PC 服务器的运行状况和健康状况，并可对异常状况进行告警。

可监控资源池中虚拟机的 CPU、内存、存储、网络实际使用情况，并可对异常状况进行报警。

可监控资源池中存储设备的使用情况。

可监控资源池中网络设备的流量信息、故障信息、告警信息，并可对异常状况进行告警。

可以展示资源的拓扑视图。

提供对于资源的自动探查功能。

提供能耗管理功能。

可以设置监控数据的保存时长，超过保存时长的数据被自动清理。

资源池系统管理员具有查看整个资源池中的资源监控信息的权限，普通管理员具有部分权限。

6.7.3 存储监控

存储设备监控，包括：

——配置管理：提供配置对象存储设备访问地址的功能、配置对象存储设备管理员账号信息的功能、配置虚拟机备份账号信息的功能、配置块存储设备访问地址的功能；

——监控管理：提供对象存储设备、块存储设备的监控功能，监控的内容包括对象存储设备和块存储设备的运行状态、存储容量等信息；

——如果块存储系统基于磁盘阵列实现，须提供对于磁盘阵列设备的监控功能；

——资源池系统管理员具有管理整个资源池中的存储设备的权限，普通管理员具有部分权限。

6.7.4 中间件监控

管理员通过中间件监控功能对资源池中间件运行状态进行整体监控，支持资源管理分平台管理员能够查看整个资源池的所有中间件的监控信息。

6.7.5 系统监控

管理员通过系统监控功能对资源池的资源或设备运行状态进行整体监控，系统监控支持资源池系统管理员能够查看整个资源池的监控信息；普通管理员具有部分权限。

6.7.6 事件管理

事件管理包括告警管理和状态报告管理。

告警管理功能完成对资源池中的告警信息的管理，包括对告警信息的查看、查询、撤销，支持告警信息的通知和提醒等功能。通过告警管理，平台管理员和系统管理员能够查看及处理整个资源池的告警

信息；平台管理员还能够将某个或某些告警信息分配至对应资源池管理员进行处理；普通管理员具有部分权限。支持自动告警处理策略和功能。

状态报告管理完成资源池状态向综合平台的上报，例如资源池运行状态、特殊状态报告等。

6.7.7 故障管理

管理员通过故障管理功能对资源池中的故障信息进行管理，包括对故障信息的查看、查询、撤销，支持故障信息的通知和提醒等功能。故障管理支持资源池系统管理员能够查看及处理整个资源池的故障信息，还能够将某个或某些故障信息分配至普通管理员进行处理。

6.8 日志管理

6.8.1 概述

操作维护日志管理，管理员通过该功能对资源池中的日志信息进行管理，包括对日志信息的查看、查询和删除。

6.8.2 操作日志及审计

用户通过虚拟化管理平台对系统所作的任意非查询类操作都需要支持记入日志，日志记录包含如下信息：

- 序号；
- 操作用户；
- 操作名称；
- 操作类型；
- 用户 IP；
- 操作描述；
- 操作时间；
- 操作结果。

操作日志支持根据过滤条件进行查询，可设置的过滤条件包括：

- 操作用户；
- 操作名称；
- 操作类型；
- 操作结果；
- 开始时间；
- 结束时间。

操作日志支持本地存储和转储，以支持回溯和审计。

6.9 统计分析

统计分析功能完成资源池的系统监控信息的统计分析。统计分析支持资源池平台管理员和系统管理员能够对整个资源池的监控信息进行统计分析；普通管理员只具有部分权限。

统计分析功能提供对系统监控信息的多维度统计分析功能，可以按照时段生成文字或图形报表以供分析。

可以统计各类资源的使用情况、可用资源情况。

可以按照统计周期进行统计分析，统计周期可配置，例如每小时、每天、每月等统计周期。

可以对统计结果按照 HTML、XML、EXCEL 等常用格式进行导出。

可以设置统计数据的保存时长，超过保存时长的数据被自动清理。

6.10 安全管理

能完成资源池的安全功能及规则的管理。支持资源池平台管理员和系统管理员能够对整个资源池的安全功能和规则进行操作，例如增加、删除、查询等。

中华人民共和国
通信行业标准
云资源管理技术要求
第3部分：分平台
YD/T 2807.3-2015

*

人民邮电出版社出版发行
北京市丰台区成寿寺路11号邮电出版大厦
邮政编码：100164
北京康利胶印厂印刷
版权所有 不得翻印

*

开本：880×1230 1/16 2015年12月第1版
印张：1.75 2015年12月北京第1次印刷
字数：46千字

15115·670

定价：20元

本书如有印装质量问题，请与本社联系 电话：(010)81055492