第3章

云计算机制

本章主要介绍常见的云计算机制，包括云基础设施机制、云管理机制和特殊云机制。通过本章的学习，读者能够对云计算的机制有所了解。

3.1 云基础设施机制

云基础设施机制是云环境的基础构件块，它是形成云技术架构基础的主要构件。云基础设施机制主要针对计算、存储、网络，包括虚拟网络边界、虚拟服务器、云存储设备和就绪环境。

这些机制并非全都应用广泛，也不需要为其中的每一个机制建立独立的架构层。相反，它们应被视为云平台中常见的核心组件。

3.1.1 虚拟网络边界

虚拟网络边界(Virtual Network Perimeter)通常是由提供和控制数据中心连接的网络设备建立，一般是作为虚拟化环境部署的。例如虚拟防火墙、虚拟网络(VLAN、VPN)。该机制被定义为将一个网络环境与通信网络的其他部分隔开，形成一个虚拟网络边界，包含并隔离了一组相关的基于云的IT资源，这些资源在物理上可能是分布式的。

该机制可被用于如下几个方面。

- 将云中的IT资源与非授权用户隔离；
- 将云中的IT资源与非用户隔离；
- 将云中的IT资源与云用户隔离；
- 控制被隔离IT资源的可用带宽。

1. 虚拟防火墙

图 3.1 是虚拟防火墙的示意图。虚拟防火墙是一个逻辑概念，该技术可以在一个单一的硬件平台上提供多个防火墙实体，即把一台防火墙设备在逻辑上划分成多台虚拟防火墙，每台虚拟防火墙都可以被看成是一台完全独立的防火墙设备，可拥有独立的管理员、安全策略、用户认证数据库等。

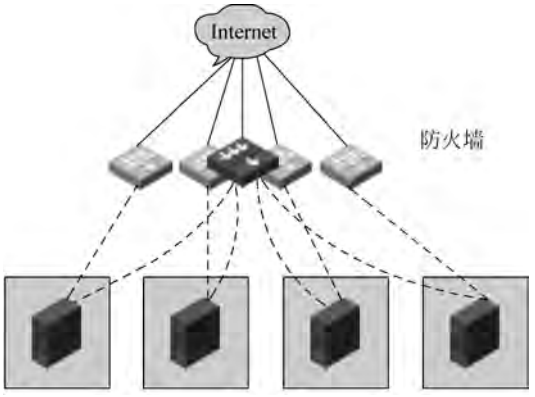

图 3.1 虚拟防火墙的示意图

每个虚拟防火墙都能够实现防火墙的大部分特性，并且虚拟防火墙之间相互独立，一般情况下不允许相互通信。

虚拟防火墙具有以下技术特点。

(1) 每个虚拟防火墙独立维护一组安全区域。

(2) 每个虚拟防火墙独立维护一组资源对象(地址/地址组、服务/服务组等)。

(3) 每个虚拟防火墙独立维护自己的包过滤策略。

(4) 每个虚拟防火墙独立维护自己的 ASPF 策略、NAT 策略、ALG 策略。

(5) 可限制每个虚拟防火墙占用的资源数，例如防火墙 Session 以及 ASPF Session 数目。

虚拟防火墙不仅解决了业务多实例的问题，更主要的是，通过它可将一个物理防火墙划分为多个逻辑防火墙使用。多个逻辑防火墙可以单独配置不同的安全策略，并且在默认情况下，不同的虚拟防火墙之间是隔离的。

2. 虚拟专用网络

虚拟专用网络(VPN)是一种通过公用网络(例如 Internet)连接专用网络(例如办公室网络)的方法。

它将拨号服务器的拨号连接的优点与 Internet 连接的方便与灵活相结合。通过使用 Internet 连接，用户可以同时在大多数地方通过距离最近的 Internet 访问电话号码连接到自己的网络。

VPN 使用经过身份验证的链接来确保只有授权用户才能连接到自己的网络，而且这

些用户使用加密来确保他们通过 Internet 传送的数据不会被其他人截取和利用。Windows 使用点对点隧道协议(PPTP)或第二层隧道协议(L2TP)实现此安全性。

图 3.2 所示为虚拟专用网络的基本原理。VPN 技术使得公司可以通过公用网络(例如 Internet)连接到其分支办事处或其他公司,同时又可以保证通信安全。通过 Internet 的 VPN 连接从逻辑上来讲相当于一个专用的广域网(WAN)连接。

图 3.2 虚拟专用网络(VPN)的基本原理

VPN 系统的主要特点如下。

(1) 安全保障:虽然实现 VPN 的技术和方式很多,但所有的 VPN 均应保证通过公用网络平台传输数据的专用性和安全性。在安全性方面,由于 VPN 直接构建在公用网上,实现简单、方便、灵活,但同时其安全问题更为突出。企业必须确保其 VPN 上传送的数据不被攻击者窥视和篡改,并且要防止非法用户对网络资源或私有信息的访问。

(2) 服务质量保证(QoS):VPN 应当为企业数据提供不同等级的服务质量保证。不同的用户和业务对服务质量保证的要求差别较大。在网络优化方面,构建 VPN 的另一重要需求是充分、有效地利用有限的广域网资源,为重要数据提供可靠的带宽。广域网流量的不确定性使其带宽的利用率很低,在流量高峰时会引起网络阻塞,使实时性要求高的数据得不到及时发送;而在流量低谷时又造成大量的网络带宽空闲。QoS 通过流量预测与流量控制策略可以按照优先级实现带宽管理,使得各类数据能够被合理地先后发送,并预防阻塞的发生。

(3) 可扩充性和灵活性:VPN 必须能够支持通过 Intranet 和 Extranet 的任何类型的数据流,方便增加新的节点,支持多种类型的传输媒介,可以满足同时传输语音、图像和数据等应用对高质量传输以及带宽增加的需求。

(4) 可管理性:从用户角度和运营商角度而言,应可方便地进行管理、维护。VPN 管理的目标为减小网络风险,具有高扩展性、经济性、高可靠性等优点。事实上,VPN 管理主要包括安全管理、设备管理、配置管理、访问控制列表管理、QoS 管理等内容。

3.1.2 虚拟服务器

服务器通常通过虚拟机监视器(VMM)或虚拟化平台(Hypervisor)来实现硬件设备的抽象、资源的调度和虚拟机的管理。虚拟服务器(Virtual Server)是一种模拟物理服务器的虚拟化软件。虚拟服务器与虚拟机(VM)是同义词,虚拟基础设施管理器(VIM)用于协调与 VM 实例创建相关的物理服务器。虚拟服务器需要对服务器的 CPU、内存、设备及 I/O 分别实现虚拟化。

通过向云用户提供独立的虚拟服务实例,云提供者使多个云用户共享同一个物理服

务器，如图 3.3 所示。

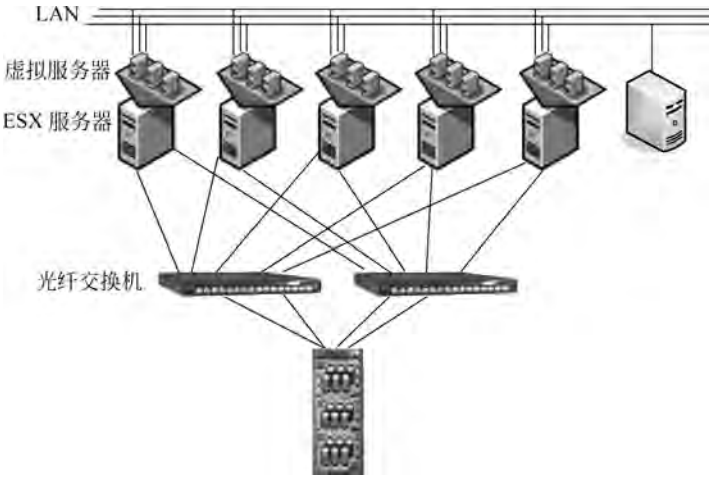

图 3.3　虚拟服务器的基本架构

每个虚拟服务器都可以存储大量的 IT 资源、基于云的解决方案和各种其他的云计算机制。从映像文件进行虚拟服务器的实例化是一个可以快速且按需完成的资源分配过程。通过安装和释放虚拟服务器，云用户可以定制自己的环境，这个环境独立于其他正在使用由同一底层物理服务器控制的虚拟服务器的云用户。虚拟服务器的具体内容将在 4.2 节详细介绍。虚拟服务器有以下几个特性。

（1）多实例：通过服务器虚拟化，一台物理机上可以运行多个虚拟服务器，支持多个客户操作系统，并且物理系统的资源是以可控的方式分配给虚拟机。

（2）隔离性：虚拟服务器可以将同一台物理服务器上的多个虚拟机完全隔离开来，多个虚拟机之间就像多个物理机器之间一样，每个虚拟机都有自己独立的内存空间，一个虚拟机的崩溃并不会影响到其他虚拟机。

（3）封装性：一个完整的虚拟机环境对外表现为一个单一的实体，便于在不同的硬件设备之间备份、移动和复制。同时，虚拟服务器将物理机器的硬件封装为标准化的虚拟硬件设备提供给虚拟机内的操作系统和应用程序，提高了系统的兼容性。

基于以上这些特性，虚拟服务器带来了如下优点。

（1）实时迁移：实时迁移是指在虚拟机运行时，将虚拟机的运行状态完整、快速地从一个宿主平台迁移到另一个宿主平台，整个迁移过程是平滑的，且对用户透明。由于虚拟服务器的封装性，实时迁移可以支持原宿主机和目标宿主机硬件平台之间的异构性。

当一台物理机器的硬件需要维护或更新时，实时迁移可以在不宕机的情况下将虚拟机迁移到另一台物理机器上，大大提高了系统的可用性。

（2）快速部署：在传统的数据中心中，部署一个应用需要安装操作系统、安装中间件、安装应用、配置、测试、运行等多个步骤，通常需要耗费十几个小时甚至几天的时间，并且在部署过程中容易产生错误。

在采用虚拟服务器之后，部署一个应用其实就是部署一个封装好操作系统和应用程

序的虚拟机,部署过程只需要复制虚拟机、启动虚拟机和配置虚拟机几个步骤,通常只需要十几分钟,且部署过程自动化,不易出错。

(3) 高兼容性:虚拟服务器提供的封装性和隔离性使应用的运行平台与物理底层分离,提高了系统的兼容性。

(4) 提高资源利用率:在传统的数据中心中,出于对管理性、安全性和性能的考虑,大部分服务器都只运行一个应用,导致服务器的 CPU 使用率很低,平均只有 5%～20%。在采用虚拟服务器之后,可以将原来多台服务器上的应用整合到一台服务器中,提高了服务器资源的利用率,并且通过服务器虚拟化固有的多实例、隔离性和封装性保证了应用原有的性能和安全性。

(5) 动态调度资源:虚拟服务器可以使用户根据虚拟机内部资源的使用情况即时、灵活地调整虚拟机的资源,例如 CPU、内存等,而不必像物理服务器那样需要打开机箱变更硬件。

3.1.3 云存储设备

云存储设备(Cloud Storage Device)机制是指专门为基于云配置所设计的存储设备。这些设备的实例可以被虚拟化。其单位如下。

- 文件(file):数据集合分组存放于文件夹中的文件里;
- 块(block):存储的最低等级,最接近硬件,数据块是可以被独立访问的最小数据单位;
- 数据集(dataset):基于表格的以分隔符分隔的或以记录形式组织的数据集合;
- 对象(object):将数据及其相关的元数据组织为基于 Web 的资源,各种类型的数据都可以作为 Web 资源被引用和存储,例如利用 HTTP 的 CRUD(Create、Retrieve、Update、Delete)操作(例如 CDMI,全称为 Cloud Data Management Interface)。

随着云存储的广泛应用(如图 3.4 所示),一个与云存储相关的主要问题出现了,那就是数据的安全性、完整性和保密性,当数据被委托给外部云提供者或其他第三方时,更容易出现危害。此外,当数据出现跨地域或国界的迁移时,也会导致法律和监管问题。

图 3.4 云存储的广泛应用

1. 用户的操作安全

当一个用户在公司编辑某个文件后,回到家中再次编辑,那么他再次回到公司时文件已是昨晚更新过的,这是理想状态下的,在很多时候用户编辑一个文件后会发现编辑有误,想取回存在公司的文件版本时,可能在没有支持版本管理的云存储中用户的副本已经被错误地更新了。同样的道理,当删除一个文件的时候,如果没有额外备份,也许到网盘回收站中再也找不到了。版本管理在技术上不存在问题,但是会加大用户的操作难度。目前的云存储服务商只有少数的私有云提供商提供有限的支持,多数情况下这种覆盖时常发生。

2. 服务端的安全操作

云存储设备早已成为黑客入侵的目标，因为设备上不仅有无穷的用户数据，而且对此类大用户群服务的劫持更是黑色收入的重要来源。也就是说，云存储设备的安全性直接影响着用户上传数据的安全。在虚拟服务器技术的支撑下，V2V(Virtual to Virtual)迁移的可靠性相当高，多数云存储厂商都预备了安全防护方案。

3.1.4　就绪环境

PaaS平台是指云环境中的应用即服务(包括应用平台、集成、业务流程管理和数据库服务)，也可以说是中间件即服务。PaaS平台在云架构中位于中间层，其上层是SaaS，其下层是IaaS，基于IaaS之上的是为应用开发(可以是SaaS应用，也可以不是)提供接口和软件运行环境的平台层服务。

就绪环境机制是PaaS云交付模型的定义组件，基于云平台，已有一组安装好的IT资源，可以被云用户使用和定制。云用户利用就绪环境机制进行远程开发及配置自身的服务和应用程序，例如数据库、中间件、开发工具和管理工具，以及进行开发和部署Web应用程序。

Oracle的共享、高效的PaaS框架如图3.5所示，其中解释了就绪环境机制的实现位于应用运行环境层(aPaaS)，为用户提供了一套完整的运行环境。

(1) iPaaS：基于SOA、ESB、BPM等架构，是云内/云与企业间的集成平台。

(2) aPaaS：共享，基于Java等应用技术架构，是应用的部署与运行环境平台。

(3) dPaaS：可灵活伸缩，是数据存储与共享平台，提供多租户环境下高效与安全的数据访问。

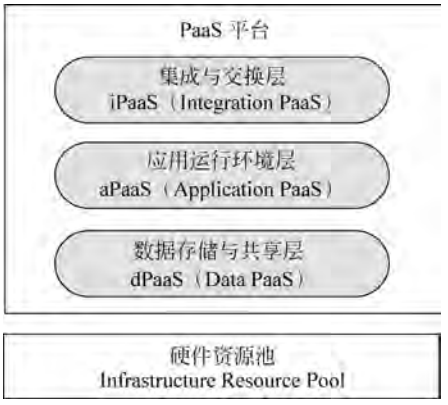

图3.5　Oracle的PaaS框架

(4) 硬件资源池：为PaaS平台提供所需要的高性能硬件资源系统。

3.2　云管理机制

云管理(CMP)这个概念的产生来源于私有云和混合云。对于企业来说，企业内部既存在传统架构，也存在云架构，采买和使用的设备以及软件厂商和型号各异，不同的企业又存在不同的环境差异，同时私有云的需求和服务也有差异，因此需要一个云管理平台，从资源池规划、服务目录管理、云CMDB、流程管控、监控容量等多个方面对数据中心进行管理和治理。

对于公有云本身来说，公有云平台已经将各种管理任务封装为标准的服务，用户在使用公有云时也会涉及管理工作，但其管理工作大多是账号管理、账单管理、权限管理等，例

如在公有云上的资源开通、架构设计、迁移等都属于服务使用范畴,使用者根据业务需求进行使用即可,不需要负责管理工作。

表 3.1 是云管理与传统管理的比较。

表 3.1 云管理与传统管理的比较

	传统管理	云管理
管理对象	网络、存储、服务器、OS、数据库、中间件、应用	IaaS、PaaS、SaaS 等各种云服务
管理目标	实现 IT 系统的正常运作	实现云服务的端对端交付及云数据中心运维
管理特色	需要专业的管理技能 手动管理 竖井式管理	通过封装屏蔽底层细节 自服务、自动化 多租户,共享管理平台
管理平台的易用性	安装配置复杂	自配置、自修复、自优化
管理规模	100 节点	10000 节点+
用户	管理员	分层管理,多租户
整合	基于事件、数据库、私有接口的整合	面向服务的整合
管理手段	离散的工具	充分自动化

经过表 3.1 所示的云管理与传统管理的比较,不难发现基于云的 IT 资源需要被建立、配置、维护和监控。远程管理系统是必不可少的,它们促进了形成云平台与解决方案的 IT 资源的控制和演化,从而形成了云技术架构的关键部分,与管理相关的机制有远程管理系统、资源池化管理、SLA 管理系统、计费管理系统、资源备份、云监控、自动化运维、服务模板管理、云 CMDB 及流程管理、服务目录管理、租户及用户管理、容量规划及管理。

3.2.1 远程管理系统

远程管理系统(Remote Administration System)机制向外部的云资源管理者提供工具和用户界面来配置并管理基于云的 IT 资源。

如图 3.6 所示,远程管理系统能建立一个入口,以便访问各种底层系统的控制和管理功能,这些功能包括资源管理、SLA(服务等级协议)管理和计费管理。

图 3.6 远程管理系统的主要功能

远程管理系统主要创建以下两种类型的入口。

(1) 使用与管理入口:一种通用入口,集中管理不同的基于云的 IT 资源,并提供资源使用报告。

(2) 自助服务入口:该入口允许云用户搜索云提供者提供的最新云服务和 IT 资源列表,然后云用户向云提供者提交其选项进行资源分配。

这个系统也包括 API,云用户可以通过这些标准 API 来构建自己的控制台。云用户可能使用多个云提供者的服务,也可能更换提供者。云用户能执行的任务如下。

- 配置与建立云服务;

- 为按需云服务提供和释放 IT 资源；
- 监控云服务的状态、使用和性能；
- 监控 QoS 和 SLA 的实行；
- 管理租赁成本和使用费用；
- 管理用户账户、安全凭证、授权和访问控制；
- 追踪对租赁服务内部与外部的访问；
- 规划和评估 IT 资源供给；
- 容量规划。

3.2.2　资源池化管理

资源池化管理系统(Resource Pool Management System)是云管理平台的关键所在，因为在一个企业内部，传统数据中心往往分散在不同地区，不同地区的数据中心也会有不同的等级以及业务属性。同时，在同一数据中心内，也会根据多个纬度进行池化划分。如图 3.7 所示，资源池是以资源种类为基础来进行划分的，因为企业环境中的硬件设备种类繁多、应用架构复杂，用户对于应用的可用性要求较高，在设计时需要充分考虑。资源池建设考虑以下 5 个因素。

图 3.7　资源池化管理系统

(1) 资源种类：企业内部存在多种异构资源，例如 x86 环境、小型机环境等，同一种类型中也存在很大差异，例如 x86 环境下的 Intel 和 AMD 处理器。在进行总体设计时，要合理规划不同种类的资源池。

(2) 应用架构：应用架构通常把应用分成多个层次，典型的格局如 Web 层、应用层、数据层和辅助功能层等，所以针对应用架构提出的层次化需求是总体设计中第二个需要考虑的因素。

(3) 应用等级保障：面对多样化的用户群体和需求，资源池需要提供不同服务等级的资源服务来满足不同的用户 SLA 需求(例如金银铜牌服务)。

(4) 管理需求：从管理角度来说，存在多种管理需求，例如高可用管理需要划分生产区、同城灾备区和异地灾备区，应用的测试、开发、培训环境，监控和日常操作管理需要划分生产区和管理操作区。

(5) 安全域：应用环境在传统网络上有逻辑隔离或者物理隔离的需求，在资源池中，需要实现同样的安全标准来保证应用正常运行。

3.2.3　服务等级协议管理系统

云计算市场在持续增长，用户如今关注的不仅仅是云服务的可用性，他们想知道厂商能否为终端用户提供更好的服务。因此，用户更关注服务等级协议(Service Level Agreement，SLA)，并需要监控 SLA 的执行情况。

服务等级协议(SLA)是服务提供者和客户之间的一个正式合同，用来保证可计量的

网络性能达到所定义的品质。

SLA 监控器(SLA Monitor)机制被用来专门观察云服务运行时性能,确保它们履行了 SLA 公布的约定 QoS 需求。例如轮询检测是否在线,检测 QoS 是否达到 SLA 的要求。

SLA 监控器保证的服务体系架构如图 3.8 所示,需要 3 个服务角色,即服务提供者、服务客户和服务代理。

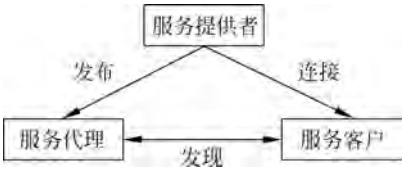

图 3.8 SLA 监控器保证的服务体系架构

首先,通过在适当的平台上创建一个 Web 服务并生成 WSDL 文档和服务的基本 SLA,服务提供者发布一个由 SLA 保证的 Web 服务。

然后,它把服务细节发送到服务代理以存储在资源库中。服务客户向代理注册,然后在代理的资源库中搜索并发现适当的 Web 服务,检索服务的 WSDL 和 SLA。

最后,它与提供者协商把 SLA 正规化,确定下来,并绑定到它的 Web 服务。

在使用 SLA 监控器机制时需要注意一些问题,例如第三方监控、告警装置、转换 SLA 以及有效的后备设施。

1. 第三方监控

审计是很重要的一步,能够确保安全,保证 SLA 的承诺和责任归属,保持需求合规。用户可以用第三方监控。如果用户在云中运行业务关键的应用,这项服务应该保证定期审查,确保合规,并督促厂商与 SLA 步调一致。

2. 转换 SLA,帮助整个业务成果

尽管云计算市场正在迅猛发展,但中小型企业的 IT 大多都不够成熟,不足以支撑基于基础设施的 SLA 来帮助业务发展。企业应该选择最适合业务需求的 SLA,而不是急急忙忙签署协议。

如果企业操之过急,直接选择基础设施级别的 SLA,可能会导致公司内部产生花费。例如,某企业想要 99.999%的高可用性,服务商就会提供更多冗余和灾难恢复,结果花费大幅度提高。

当聚焦于节俭型业务级别的 SLA 时,云计算 SLA 监控应该具有逻辑性和可行性,而不仅仅是基础设施级别的 SLA。

3. 确保告警装置

为了让 SLA 监控更高效,用户要确保可以通过 Web 门户定期报告可用性和责任时间。用户应该保证及时的 Email 告警。

4. 确保厂商有高效的后备设施

不同的厂商对于数据保护的责任分配不同,有的厂商会把责任推给客户,这样客户只好自己保护数据。因此,用户应该确定服务商在签署 SLA 时是否对此负有责任。

3.2.4　计费管理系统

计费管理系统(Billing Management System)机制专门用于收集和处理使用数据,它涉及云提供者的结算和云用户的计费。计费管理系统依靠按使用付费监控器来收集运行时使用的数据。这些数据存储在系统组件的一个库中,然后为了计费、报告和开发票等,从库中提取数据。图 3.9 是一个由定价与合同管理器和按使用付费测量库构成的计费管理系统。

图 3.9　计费管理系统的组成

3.2.5　资源备份

图 3.10 和图 3.11 分别是传统 IT 架构视角和云计算架构视角的展示。与传统 IT 架构视角不同的是,云计算集中部署计算和存储资源,提供给各个用户,这既避免了用户重复建设信息系统的低效率,又能赋予用户价格低廉且近乎无限的计算能力。云计算提供的资源是弹性可扩展的,可以动态部署、动态调度、动态回收,以高效的方式满足业务发展和平时运行峰值的资源需求。云计算使用了资源备份容错、计算节点同构可互换等措施来保障服务的高可靠性和专业的维护队伍。

图 3.10　传统 IT 架构视角

图 3.11　云计算架构视角

资源备份(Resource Backup)可对同一个 IT 资源创建多个实例。资源备份用于加强 IT 资源的可用性和性能。使用虚拟化技术来实现资源备份机制,可以复制基于云的 IT 资源(例如整个数据中心中的应用、数据)实现集中的备份和恢复,确保当出现系统故障、误操作等时应用系统仍然可用和可恢复。

对于私有数据中心或私有云平台来说,企业可以利用云存储的能力实现云端备份,这样可以降低不可抗力因素造成数据丢失的风险。主流的公有云厂商都提供了云端备份方案,例如可以把数据库镜像或者文件系统中的文件批量备份到云端,也可以在云端启动数据库实例的副本,并实时复制数据。

对于公有云平台,本身就提供了异地多副本备份机制,可以将数据库快照复制到另外

一个可用区或者其他区域进行备份。同时,对于数据库的备份,也可以选择在启动一个数据实例时对该实例进行多区域的部署。

3.2.6 云监控

云资源监控是为了保证应用和服务的性能,开发者必须依据应用程序、服务的设计和实现机制估算工作负载,确定所需资源和容量,避免资源供应不足或供应过量。

虽然负载估计值可通过静态分析、测试和监控得到,但实际上系统负载变化迅速、难以预测。云提供商通常负责资源管理和容量规划,提供 QoS 保证。因此,监控对于云提供商是至关重要的。提供商根据监控信息追踪各种 QoS 参数的变化,观察系统资源的利用情况,从而准确规划基础设施和资源,遵守 SLA。

在私有云和混合云中,云监控主要是管理员对云环境进行监控管理以及以用户自服务方式进行监控管理。在公有云中,通常不涉及管理员部分的监控,多为以用户自服务方式对自己开通的资源进行监控。

在私有云中,管理员应该可以通过云监控平台获取基础架构资源信息,通过仪表板和报告的方式掌握云平台的资源使用情况。云平台可以发现所有开通的虚拟机以及资源使用情况;自动提供虚拟资源和物理资源的映射,便于发现虚拟资源和物理资源的关系;监控集群、资源池、虚拟主机、具体虚拟机的运行情况,监控的指标涵盖了运行状态、存储、网络、CPU、内存等各方面的性能和状态参数。

在企业内往往遗留了一部分传统非云架构,所以需要企业内的私有云平台可以监控云化以及非云的资源。除了基础架构资源外,有些企业管理员还担负基础架构上层的应用资源监控的职责,例如数据库连接池状态、MQ 消息队列状态等。

云监控可以让用户及管理员自己设置监控阈值,当资源使用低于阈值时,自动产生告警并发送到事件告警平台,方便管理员统一查看管理。

从管理员的角度而言,云平台的监控是对云数据中心的监控,这里包括了物理环境监控、虚拟化环境监控、操作系统及组件监控、业务影响分析等。除此之外,对于支撑云数据中心的机房本身也需要做监控管理。

通常,一个云管理平台面向管理员的监控系统应涵盖以下内容。

- 数据采集:数据采集可采用多种类型的采集模式,例如 Webservice、文件接口(FTP)、DB-Link、Socket、CORBA、RMI、CWMP 消息队列等。信息采集接口方式与信息模型松耦合,即无论采取何种接口方式或技术,其交互的信息都应遵循统一的信息模型。采集类别包括容量数据、性能数据、网络监控数据、操作监控数据、应用监控数据、日志数据。
- 数据处理和分析:能够对收集的数据进行加工处理,发掘其内在规律,为运行决策提供支持;具备对接现有各个数据库的能力,提供网络运行、容量管理、运维流程、业务运行情况等综合性数据分析服务;提供性能动态基线功能,能够根据业务和系统运行规律的变化趋势自动学习各个性能指标特点,加权计算出动态基线,包含小时、周天、周末、日期等基线,以此基线作为动态阈值。
- 告警事件管理:监控平台能够对云平台的告警事件进行统一管理,对事件进行过

滤、压缩、相关性分析、自动化处理、报警升级等工作，建立高效、易用、灵活的事件管理。监控平台自身具有良好的事件分析处理功能，必须使用独立的分析引擎，为了保证在出现事件风暴的情况下事件处理核心不崩溃，需要提供告警事件处理功能，可以对实时告警事件信息进行采集，根据管理需要进行信息过滤、关联、重复事件压缩、事件关联分析和处理，并将这些信息分发给负责处理的管理员；能够对大事件量进行采集和处理，以支持现在的管理需要和未来的管理扩展。

云计算是对既有的计算资源在一种全新模式下的重组。在云端，数以万计的服务器提供近乎无穷的计算能力，而云用户根据自己的需求获取相应的计算能力。集中的存储和计算形成了云能耗黑洞。云计算系统作为未来信息通信系统中内容与服务的源头与处理核心，也已成为信息通信系统的能耗大户。现在，能量支出已经成为云计算系统运营不断增加的成本，有可能超过购买硬件资源的成本。为了充分利用能量，提供系统能效，降低能量成本，需要从监控能耗入手，利用采集来的系统运营状态参数对服务器中的主要耗能部件进行建模分析，为节能策略的构建提供依据。

云计算是一种按使用量付费的模式，使用付费监控器(Pay-per-Use Monitor)机制按照预先定义好的定价参数测量基于云的 IT 资源使用，使用期间生成的日志可以计算费用，日志主要包括请求/响应消息数量、传送的数据量、带宽消耗量。

3.2.7 自动化运维

在传统数据中心中，将开发好的业务交给运维人员，运维人员要保证其可用性，通常从服务器、网络、存储、应用几个方面进行运维和管理。在自动化运维中，也可以从这几个角度进行运维和管理。

在上了云平台之后，云平台本身有资源集中和资源上收的要求，IT 组织面临众多挑战，例如不断增加的复杂性、成本削减要求、合规要求以及更快响应业务需求的压力。许多 IT 组织艰难地应对这些挑战，并承认目前的运营方法根本无法让他们取得成功。手动操作具有被动性，需要大量人工，容易出错，而且严重依赖高素质人员。同时，通过单点解决方案或基于脚本的方法也难以解决手工运维的种种问题，企业开始转而寻找能够利用一个集成式平台来满足其所有服务器管理与合规需求的综合解决方案。

云平台可以集成配置自动化与合规保证的独特架构，使 IT 组织能够实施基于策略的自动化解决方案来管理其数据中心，同时确保其关键业务服务的最大正常运行时间。另外，由于用户继续采用虚拟化和基于云计算的技术，服务器自动化运维为跨越所有主要虚拟平台管理物理和虚拟服务器提供了单一平台。在可靠、安全模型的支持下，该解决方案使企业能够通过满足其在配置、指配和合规 3 个领域的需求而大大降低运营成本，提高运营质量和实现运营合规。

那么运维自动化应涵盖哪些方面呢？自动化开通资源本身就解决了从手动到自动的资源创建过程。那么在资源创建后呢？在资源创建后，更多时间是如何进行运维和保障，而在弹性自服务方式开通时，用户所面对的资源是呈几何倍数增长的。在这种情况下，云平台的自动化运维就显得格外重要，可以从以下几个方面考虑运维的自动化，应该注意云平台本身涉及很多自动化技术，本节主要说明对于管理员端该如何自动化运维以及考虑

的方面。

(1) 配置：配置管理任务在数据中心执行的活动中通常占有相当高的比例，包括服务器打补丁、配置、更新和报告。通过对用户隐藏底层复杂性，云平台能够确保变更和配置管理活动的一致性。同时，在安全约束的范围内，它可以提供关于被管理服务器的足够的详细信息，从而确保管理活动的有效和准确。

(2) 合规：大多数 IT 组织都需要使其服务器配置满足一些策略的要求，不管是监管(SOX、PCI 或 HIPAA)、安全(NIST、DISA 或 CIS)还是运营方面。云平台应该可以帮助 IT 组织定义和应用配置策略，从而实现并保持合规。当某个服务器或应用程序配置背离策略时，它会自动生成并打包必要的纠正指令，而且这些指令可以自动或手动部署在服务器上。

(3) 补丁：云平台的自服务往往会让管理员担心服务器成倍增长带来的可控性，尤其是漏洞给企业的生产安全带来的隐患。云平台给管理员提供便捷的补丁自动下载、自动核查现有操作系统补丁状态、自动安装和出具报告等功能，对于不同平台的操作系统，都可以实现联网，自动获取补丁库。

(4) 自动发现：对于弹性云环境，资源变化相当频繁，包括主机漂移等，都会给企业的资产维护带来不确定性，尤其是运维人员想了解当下哪些服务器装了哪些操作系统及其版本，以及上面运行的组件软件(包括组件间访问关系)等，这些都给运维人员对资产的了解提出了挑战。因此，云平台运维应该可以自动扫描基础架构，能发现服务器、网络、存储的配置信息，并可以自动生成应用组件拓扑。

3.2.8 服务模板管理

服务模板管理也可以理解为服务蓝图。服务蓝图给出了一种可视化、架构式定义服务的全新方式。

(1) 提供服务的部署视图：定义部署服务的一种或多种方式(例如虚拟部署形态、物理部署形态，甚至公有云部署形态)。

(2) 能够说明服务运行所需的资源。

(3) 由服务器对象、存储对象和网络对象(含负载均衡/防火墙规则)组成。

服务设计器支持服务组装，以拖曳方式将软件包、操作系统、网络配置定义等原子服务组合为包含多个服务节点并相互关联的复杂服务。底层调度引擎自动根据服务设计器生成的服务描述驱动资源层自动化模块完成服务的创建与配置，无须人工干预。

服务蓝图的构成包括组件定义、组件 OS，以及软件定义、网络配置定义等。通过服务蓝图可以简化服务的维护，并对各服务组成方式进行单独、无耦合的管理和实现。特别地，当未来需要增加新的部署模式时，需要新的“集群环境(集群部署架构)”时，仅需要对该部署模式进行定义，并挂接到同一个服务蓝图下。松耦合的服务定义方式大大提高了服务管理的能力。

同时，服务蓝图的参数化支持服务前端的高度灵活性。例如在服务蓝图中可以将数据库组件的数据库实例名及服务端口参数化，这样前端用户就可以在请求该服务时输入期望的值。服务蓝图的管理方式分割了后端实现与前端界面的紧密依赖。事实上，该参

数化在服务蓝图上实现后，平台将自动对接更低层的资源管理层，以实现资源部署时的动态逻辑，即在用户请求被确认后，平台发起数据库部署时，动态地将用户给定的值传入，作为创建的数据库服务的实例名和服务端口。基于服务蓝图的特性，用户具备了实现端到端灵活化服务的能力。

3.2.9 云 CMDB 及流程管理

CMDB(Configuration Management Database，配置管理数据库)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紧密相连，支持这些流程的运转，发挥配置信息的价值，同时依赖于相关流程保证数据的准确性。在实际项目中，CMDB 常常被认为是构建其他 ITIL 流程的基础而优先考虑，ITIL 项目的成败和是否成功建立 CMDB 有非常大的关系。在云数据中心中对 CMDB 提出了新的要求，大家知道，每个 IaaS 都有一个自己的 CMDB，那么如何实现对 IaaS 云的 CMDB 管理？Docker 和其他类似服务化平台出现之后，又如何实现对这类资源的管理？

当云到来的时候，传统的 CMDB 依然显示出其重要作用，对于资源管理的核心环节，需要对企业内部形成统一台账。本节并不想通过过多的篇幅来讲述 CMDB 本身，而只是对在云平台下，如何能够对动态的基础架构信息进行数据管理做一个简单的思路介绍。

和过去的传统运维方式不同，传统方式下的资源发放都是用户提交申请，然后管理员手动开通的，而在手动开通中，管理员是可以对该开通的资源进行表单记录和 CI 项录入的。但是在云环境下，资源都是用户以自助方式开通，同时对于资源配置的修改，例如纵向扩容增减资源，或者虚拟机漂移等，都会对 CI 项产生影响。

在云平台中，通过自服务开通的这些云资源项(包括虚拟化平台本身以及虚拟化架构、虚拟化架构中的各种配置信息)都需要进行数据填充形成 CI 项，而这些如果通过手动完成，几乎是不可能的，因此需要借助自动发现的能力，自动发现动态中的云环境资源信息，同时自动搜集出 CI 项，填充到 CMDB 中。用户可以为云环境中的 CI 项单独配置一个沙箱，除了从云平台本身自动发现的数据以外，还有业务系统自动产生的一些数据，这些数据可以进行调和，并形成一个准确的 CI 项录入 CMDB。

3.2.10 服务目录管理

无论是在公有云上或者企业私有云上看到的服务或者目录，都是从用户角度看到的。管理员该如何对服务目录进行定义？如果要构建云平台的服务目录，应该具备什么样的能力？下面做一下简单介绍。

(1) 服务目录应该支持对服务的生命周期管理：提供对云服务全生命周期的管理，服务的创建、申请、变更、审批、修改、发布、授权及回收等过程在一个统一的云管理平台上实现。服务创建后可由云平台管理员进行发布。服务发布是对服务库和服务目录中的服务在运营管理系统内进行变更、激活、挂起、撤销等过程的管理。用户只可对发布状态为激活并经过授权的服务进行请求。

(2) 服务目录定义了 IT 服务的使用者与 IT 资源之间的标准接口：管理员在服务目录中可以定义、发布、更新和终止 IT 服务，对 IT 服务的名称、描述、资源类别、资源规模、

费用等做出规定,同时可以设定不同用户访问服务目录的权限。管理员可以在服务目录中定义计费策略,包括服务中的选项以及选项内容;设计计量标准,例如 CPU、内存等不同实例对应的价格,不同性能磁盘对应的计量、计价等。

(3) 服务实例的管理:提供针对服务实例管理的用户界面,支持对服务实例的创建、审批、变更、终止等操作,管理员能够对服务实例的基本信息、服务请求流程的执行状态等进行操作与查询;支持用户提交修改资源配置的申请,例如 CPU 个数、内存大小等。用户可针对已有的服务实例提交软件安装或补丁安装申请,例如申请自动安装数据库软件或为某个软件自动打补丁。用户可针对已有的服务实例提交增加或删除虚拟网卡的需求,可指定网卡所在的网络。另外,用户可针对已有的服务实例提交增加或删除磁盘的需求。

(4) 审批设定:针对不同的服务设计流程审批模板。审批管理可以根据用户的请求决定所需要的审批流程,该流程可以是串行、并行,或者单级、多级等模式,支持委托代理审批。管理员可以批准用户的申请,也可以拒绝用户的申请。在审批过程中需要留下详细的审计记录。如果服务申请被批准或拒绝,在自动化操作完后,将自动给申请人以及相关人员发邮件通知。

3.2.11 租户及用户管理

云平台与传统系统一样,都需要涉及租户和用户的管理。私有云通常叫租户管理,而在公有云中通常叫 Account 或者 Organization。对于租户管理,云平台允许创建租户,并且第一个创建该租户的具有管理员的角色。对于不同租户的资源和数据隔离,通常可以通过 VPC 逻辑区分,然后再通过 VPC 和相应的网络安全策略进行绑定,从而实现逻辑隔离。

除了租户外,还需要设计权限和用户以及用户组,权限可以赋予用户组,也可以单独赋予某个用户,通过用户组可以更方便地划分用户属性。通过用户组合角色绑定,可以对用户所能看到的页面信息和访问视图进行控制。

在私有云中还会涉及配额管理,在公有云中不会涉及。这主要因为公有云对服务的申请会生成账单,而私有云往往用户申请资源,属于内部核算,不会发生真正的费用,因此需要指定配额,从而对租户以及用户进行使用量的限制。对用户可以设置资源使用额度,包括该用户所能申请的最大 CPU、内存、磁盘和申请的云主机数量的额度。当申请额度达到上限时无法继续申请资源,需要重新调整额度,然后才能申请。云平台管理员可以设置租户管理员额度,租户管理员可以设置租户内用户额度。额度可以设置为无限量。

3.2.12 容量规划及管理

云平台对容量的考量是非常有必要的,无论是公有云还是私有云。云端资源申请是弹性的、动态的,那么管理员什么时候知道该扩容?扩哪里?扩什么资源呢?在这个时候就需要云管理平台具备容量分析和规划的能力。

容量规划是基础设施运维服务的重要组成部分,业务关联度高,整合性强,预测误差小的容量预测工具能够有效预测资源池性能瓶颈和发生的时间点,避免性能问题所造成

的服务中断。同时，容量信息也是硬件采购、系统扩容以及节能减排等工作的重要依据。

容量管理和规划需要具备分析、预测的能力，具备良好的数据兼容性，能够从网络、服务器、数据库、中间件、业务等监控系统中抽取指定的性能数据，并以直观的方式呈现给容量分析人员。同时系统内置预测/分析模块，支持 what-if、时间序列等分析模式，并绘制资源/服务趋势预测图，出具容量分析和规划报表。

系统支持业务场景下的容量分析。系统能够同时对资源指标、服务指标以及业务指标进行关联度分析与预测，并提供相应的 what-if 预测，包括如下内容。

(1) 指定业务 KPI，分析特定条件下的容量需求，例如访问量增加 30%，保证在系统响应时间不变的条件下系统的可能瓶颈点以及容量需求。

(2) 指定业务 KPI，分析系统的最大业务容量，保证在系统响应时间不变的条件下当前系统能支持的最大并发用户数。

(3) 分析基础设施扩容，包括水平及垂直扩展，以及业务增长趋势对资源利用率、业务 KPI 的影响。

(4) 标识可能的性能瓶颈点，例如为了保证响应的时间，当业务量增加 30%，标识此时系统的性能瓶颈点。

(5) 根据 SPEC、TPC-C 等机构发布的硬件规格(Hardware Benchmarks)评估，比较不同的硬件对系统容量的影响，支持定制化 Benchmarks。

(6) 提供容量面板、分析与规划报表。

3.3 特殊云机制

典型的云技术架构包括大量灵活的部分，这些部分应对 IT 资源和解决方案有不同的使用要求。通常有如下特殊云机制。

- 自动伸缩监听器；
- 负载均衡器；
- 故障转移系统；
- 虚拟机监控器；
- 资源集群；
- 多设备代理；
- 状态管理数据库。

用户可以把这些机制看成对云基础设施的扩展。

3.3.1 自动伸缩监听器

自动伸缩监听器(Automated Scaling Listener)机制是一个服务代理，它监听和追踪用户与云服务之间的通信或 IT 资源的使用情况。实际上就是监听，如果发现超过阈值(大或者小，例如 CPU＞70%，用户请求每秒大于 10 个，并持续 10 分钟)，通知云用户(VIM 平台)，云用户(VIM 平台)可以进行调整。注意，这只是监听器监听自动伸缩的需求，不是处理自动伸缩。如果扩展需求在同一物理服务器上无法实现，则需要 VIM 执行

虚拟机在线迁移,迁移到满足条件的另一台物理服务器上。

对于不同负载波动的条件,自动伸缩监控器可以提供不同类型的响应,例如:

(1) 根据云用户实现定义的参数,自动伸缩 IT 资源。

(2) 当负载超过当前阈值或低于已分配资源时,自动通知云用户。

3.3.2 负载均衡器

负载均衡器(Load Balancer)机制是一个运行时代理,有下面 3 种方式,它们都是分布式的,而不是主/备(备份)的方式。该机制可以通过交换机、专门的硬件/软件设备以及服务代理来实现。

- 非对称分配(asymmetric distribution):较大的工作负载被送到具有较强处理能力的 IT 资源。
- 负载优先级(workload prioritization):负载根据其优先级别进行调度、排队、丢弃和分配。
- 上下文感知的分配(content-aware distribution):根据请求内容分配到不同的 IT 资源。

负载均衡器被程序编码或者被配置成含有一组性能以及 QoS 规则和参数,一般目标是优化 IT 资源使用,避免过载并最大化吞吐量。负载均衡器机制可以是多层网络交换机、专门的硬件设备、专门的基于软件的系统、服务代理。

负载均衡的实现方式有以下几类。

1. 软件负载均衡技术

该技术适用于一些中小型网站系统,可以满足一般的均衡负载需求。软件负载均衡技术是在一个或多个交互的网络系统中的多台服务器上安装一个或多个相应的负载均衡软件来实现的一种均衡负载技术。

软件可以很方便地安装在服务器上,并且实现一定的均衡负载功能。软件负载均衡技术配置简单、操作方便,最重要的是成本很低。

2. 硬件负载均衡技术

由于硬件负载均衡技术需要额外增加负载均衡器,成本比较高,所以适用于流量高的大型网站系统。不过对于目前较有规模的企业网站、政府网站来说,都会部署硬件负载均衡设备,原因是一方面硬件设备更稳定,另一方面也是合规性达标的目的。

硬件负载均衡技术是在多台服务器间安装相应的负载均衡设备,也就是通过负载均衡器来完成均衡负载技术,与软件负载均衡技术相比,能达到更好的负载均衡效果。

3. 本地负载均衡技术

本地负载均衡技术是对本地服务器集群进行负载均衡处理。该技术通过对服务器进行性能优化,使流量能够平均分配在服务器集群中的各个服务器上。本地负载均衡技术不需要购买昂贵的服务器或优化现有的网络结构。

4. 全局负载均衡技术

全局负载均衡技术(也称为广域网负载均衡)适用于拥有多个服务器集群的大型网站系统。全局负载均衡技术是对分布在全国各个地区的多个服务器进行负载均衡处理,该技术可以通过对访问用户的 IP 地理位置的判定,自动转向地域最近点。很多大型网站都使用这种技术。

5. 链路集合负载均衡技术

链路集合负载均衡技术是将网络系统中的多条物理链路当作单一的聚合逻辑链路来使用,使网站系统中的数据流量由聚合逻辑链路中所有的物理链路共同承担。这种技术可以在不改变现有的线路结构、不增加现有带宽的基础上大大提高网络数据吞吐量,节约成本。

3.3.3 故障转移系统

故障转移系统(Failover System)通过集群技术提供冗余实现 IT 资源的可靠性和可用性。故障转移集群是一种高可用的基础结构层,由多台计算机组成,每台计算机相当于一个冗余节点,整个集群系统允许某部分节点掉线、故障或损坏,而不影响整个系统的正常运作。

一台服务器接管发生故障的服务器的过程通常称为“故障转移”。如果一台服务器变为不可用,则另一台服务器自动接管发生故障的服务器并继续处理任务。集群中的每台服务器在集群中至少有一台其他服务器确定为其备用服务器。故障转移系统有以下两种基本配置。

- 主动-主动:IT 资源的冗余实现会主动地同步服务工作负载,失效的实例从负荷均衡调度器中删除(或置为失效)。
- 主动-被动:有活跃实例和待机实例(无负荷,可最小配置),如果检测到活跃实例失效,将被重定向到待机实例,该待机实例就成为了活跃实例。原来的活跃实例如果恢复或者重新建立,可成为新的待机实例。这就是冗余机制。

负载均衡是对新请求进行保护,对于正在处理的请求(或者请求组)是会丢失的。至于采用哪种方式,由具体业务特性决定。

如图 3.12 所示,第一台服务器(Database01)是处理所有事务的活动服务器,仅当 Database01 发生故障时,处于空闲状态的第二台服务器(Database02)才会处理事务。故障转移集群将一个虚拟 IP 地址和主机名(Database10)在客户端和应用程序所使用的网络上公开。

3.3.4 资源集群

资源集群(Resource Cluster)将多个 IT 资源实例合并成组,使之能像一个 IT 资源那样进行操作,也就是 N in 1。在实例间通过任务调度、数据共享和系统同步等进行通信。集群管理平台作为分布式中间件,运行在所有的集群节点上。资源集群的类型如下。

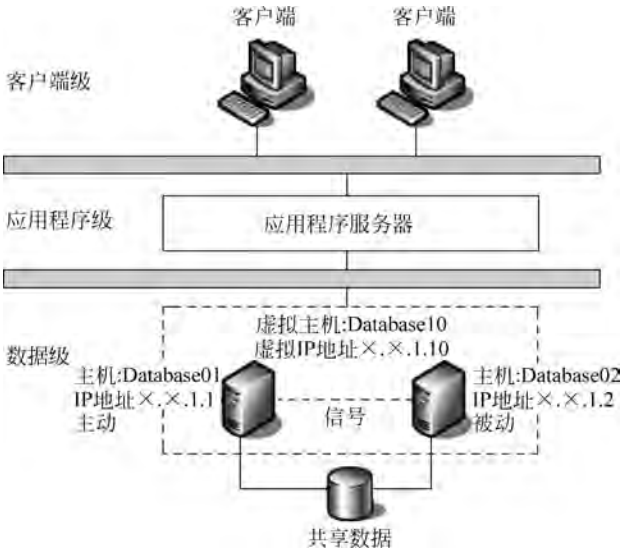

图 3.12 故障转移系统的工作原理

- 服务器集群：运行在不同物理服务器上的虚拟机监控器可以被配置为共享虚拟服务器执行状态(例如内存页和处理器寄存器状态)，以此建立起集群化的虚拟服务器，通常需物理服务器共享存储，这样虚拟服务器就可以从一个物理服务器在线迁移到另一个。
- 数据库集群：具有同步的特性，集群中使用的各个存储设备上存储的数据一致，提供冗余能力。
- 大数据集集群(Large Dataset Cluster)：实现数据的分区和分布，目标数据集可以有效地花费区域，而不需要破坏数据的完整性或计算的准确性。每个节点都可以处理负载，而不需要像其他类型那样，与其他节点进行很多通信。

其中，HA 集群是资源集群的一种，Linux-HA 的全称是 High-Availability Linux，它是一个开源项目。这个开源项目的目标是通过社区开发者的共同努力，提供一个增强 Linux 可靠性(Reliability)、可用性(Availability)和可服务性(Serviceability)的集群解决方案。

Heartbeat 是 Linux-HA 项目中的一个组件，也是目前开源 HA 项目中最成功的一个例子，它提供了所有 HA 软件需要的基本功能，例如心跳监测和资源接管、监测集群中的系统服务、在集群中的节点间转移共享 IP 地址的所有者等。其中涉及节点、资源、事件和动作 4 个相关术语。

1. 节点(Node)

运行 Heartbeat 进程的一个独立主机称为节点，节点是 HA 的核心组成部分，每个节点上运行着操作系统和 Heartbeat 软件服务。在 Heartbeat 集群中节点有主次之分，分别称为主节点和备用/备份节点，每个节点拥有唯一的主机名，并且拥有属于自己的一组

资源，例如磁盘、文件系统、网络地址和应用服务等。在主节点上一般运行着一个或多个应用服务，而备用节点一般处于监控状态。

2. 资源（Resource）

资源是一个节点可以控制的实体，并且当节点发生故障时，这些资源能够被其他节点接管。在 Heartbeat 中，可以当作资源的实体有如下几种。

- 磁盘分区、文件系统；
- IP 地址；
- 应用程序服务；
- NFS 文件系统。

3. 事件（Event）

事件就是集群中可能发生的事情，例如节点系统故障、网络连通故障、网卡故障、应用程序故障等。这些事件都会导致节点的资源发生转移，HA 的测试也是基于这些事件进行的。

4. 动作（Action）

事件发生时 HA 的响应方式，动作是由 Shell 脚本控制的。例如，当某个节点发生故障后，备份节点将通过事先设定好的执行脚本进行服务的关闭或启动，进而接管故障节点的资源。

图 3.13 是一个 Heartbeat 集群的一般拓扑图。在实际应用中，由于节点的数目、网络结构、磁盘类型配置不同，拓扑结构可能会有所不同。在 Heartbeat 集群中，最核心的是 Heartbeat 模块的心跳监测部分和集群资源管理模块的资源接管部分，心跳监测一般由串行接口通过串口线来实现，两个节点之间通过串口线相互发送报文来告诉对方自己当前的状态，如果在指定的时间内未收到对方发送的报文，那么就认为对方失效，这时资源接管模块将启动，用来接管运行在对方主机上的资源或者服务。

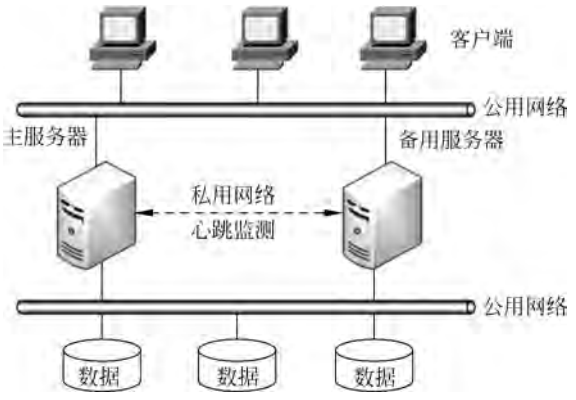

图 3.13　Heartbeat 集群的一般拓扑图

3.3.5 多设备代理

多设备代理(Multi-Device Broker)机制用来帮助运行时的数据转换,使得云服务被更广泛的用户程序和设备所用。

多设备代理通常是作为网关存在的,或者包含有网关的组件,例如 XML 网关、云存储网关、移动设备网关。

用户可以创建的转换逻辑层次包括传输协议、消息协议、存储设备协议、数据模型/数据模式。

3.3.6 状态管理数据库

状态管理数据库(State Management Database)是一种存储设备,用来暂时地存储软件的状态数据。作为把状态数据缓存在内存中的一种替代方法,软件程序可以把状态数据卸载到数据库中,用于降低程序占用的运行时内存量。因此,软件程序和周边的基础设施都具有更大的可扩展性。

3.4 小结

基础机制是指在 IT 行业内确立的具有明确定义的 IT 构件,它通常区别于具体的计算模型和平台。云计算具有以技术为中心的特点,这就需要建立一套正式机制作为探索云技术架构的基础。本章介绍了云计算中常用的云计算机制,在实现过程中可以将它们组成不同的组合形式来具体应用。

3.5 习题

1. 云基础设施机制包括哪些?
2. 云管理机制包括哪些?
3. 特殊云机制包括哪些?