第 3 章 理解云计算

（云计算是分布式计算的一种特殊形式，它引入效用模型来远程供给可扩展和可测量的资源）

云计算是一种模型，可以实现随时随地、便捷地、按需地从可配置计算资源共享池中获得所需的资源（例如，网络、服务器、存储、应用程序及服务），资源可以快速供给和释放，使管理工作量和服务提供者的介入降低至最少。这种云模型由五个基本特征、三种服务模型和四种部署模型构成

虚拟化是一个技术平台，用于创建 IT 资源的虚拟实例。虚拟化软件层允许物理 IT 资源提供自身的多个虚拟映像，这样多个用户就可以共享它们的底层处理能力

体现了云计算需求并导致其形成的主要商业驱动力：容量规划、降低成本和组织灵活性

影响并启发了云计算关键特征的主要技术创新：集群技术、网格计算和传统虚拟化技术

云是指一个独特的 IT 环境，其设计目的是为了远程供给可扩展和可测量的 IT 资源

IT 资源是指一个与 IT 相关的物理或虚拟的事物，它既可以是基于软件的，比如虚拟服务器或定制软件程序，也可以是基于硬件的，比如物理服务器或网络设备

从 IT 资源的角度来看，可扩展是指 IT 资源可以处理增加或减少的使用需求的能力，可扩展主要有两种类型：水平扩展和垂直扩展

分配和释放 IT 资源都属于水平扩展，水平分配资源也称为向外扩展，水平释放资源也称为向内扩展

当一个现有 IT 资源被具有更大或更小容量的资源所代替，则为垂直扩展，被具有更大容量的 IT 资源代替，称为向上扩展，被具有更小容量的 IT 资源代替，称为向下扩展

云服务是指任何可以通过云远程访问的 IT 资源

云服务用户是一个临时的运行时角色，由访问云服务的软件程序担任

可用性更高的 IT 资源具有更长的可访问时间

具有更强可靠性的 IT 资源能更好地避免意外情况，或是从中更快恢复

云的五个基本特征：降低的投资与成比例的开销、提高的可扩展性、提高的可用性和可靠性

第四章 基本概念与模型

提供基于云的 IT 资源的组织机构称为云提供者

云用户是组织机构（或者人），它们与云提供者签订正式的合同或者约定来使用云提供者提供的可用的 IT 资源

在法律上拥有云服务的个人或者组织称为云服务拥有者，云服务拥有者可以是云用户，或者是拥有该云服务所在的云的云提供者

当云用户在云中部署了自己的服务，它就变成云服务拥有者；如果云提供者部署了自己的云服务，通常是供其他云用户来使用的，它就变成了云服务拥有者

云资源管理者是负责管理基于云的 IT 资源（包括云服务）的人或者组织。云资源管理者可以是（或者说属于）云服务所属的云的云用户或云提供者，云资源管理者也可以是（或者说属于）签订了合约来管理基于云的 IT 资源的第三方组织

组织边界是一个物理范围，包括由一家组织拥有和管理的 IT 资源的集合

信任边界是一个逻辑范围，通常会跨越物理边界，表明 IT 资源受信任的程度

云环境的特性：按需使用、随处访问、多租户（和资源池）、弹性、可测量的使用、可恢复性

一个软件程序的实例能够服务不同的用户（租户），租户之间是互相隔离的，使得软件程序具有这种能力的特性称为多租户

弹性是一种能力，云根据运行时条件或云用户或云提供者事先确定的要求，自动透明地扩展 IT 资源

可测量的使用特性表示的是云平台记录对 IT 资源使用情况的能力

可恢复计算是一种故障转移的形式，它在多个物理位置分放 IT 资源的冗余实现。在云计算里，可恢复性特性可以是指在同一云中（但不同物理位置上）的冗余 IT 资源，也可以是跨越多个云的冗余 IT 资源

云交付模型是云提供者提供的具体的、事先打包好的 IT 资源组合。公认的和被形式化描述了的三种常见云交付模型是：基础设施作为服务（IaaS）、平台作为服务（PaaS）、软件作为服务（SaaS）

IaaS 交付模型是一种自我包含的 IT 环境，由以基础设施为中心的 IT 资源组成，可以通过基于云服务的接口和工具访问和管理这些资源。这些环境可以包括硬件、网络、连通性、操作系统以及其他一些“原始的”IT 资源

PaaS 交付模型是预先定义好的“就绪可用”的环境，一般由已经部署好和配置好的 IT 资源组成

SaaS 通常是把软件程序定位成共享的云服务，作为“产品”或通用的工具进行提供

云交付模型	赋予云用户的典型控制等级	云用户可用的典型功能	常见的云用户行为	常见的云提供者行为

SaaS	使用和与使用相关的配置	前端用户接口访问	使用和配置云服务	实现、管理和维护云服务，监控云用户的使用
PaaS	有限的管理	对与云用户使用平台相关的IT资源的中等级级别的管理控制	开发、测试、部署和管理云服务以及基于云的解决方案	实现配置好的平台和在需要时提供底层的基础设施、中间件和其他所需的IT资源，监控云用户的使用
IaaS	完全的管理	对虚拟化的基础设施相关的IT资源以及可能的底层物理 IT资源的完全访问	建立和配置裸的基础设施，安装、管理和监控所需的软件	提供和管理需要的物理处理器、存储、网络和托管，监控云用户的使用

云部署模型表示的是某种特定的云环境类型，主要是以所有权、大小和访问方式来区别的，有四种常见的云部署模型：公有云、社区云、私有云、混合云

公有云是由第三方提供者拥有的可公共访问的云环境，公有云里的 IT 资源通常是按照实现描述好的云交付模型提供的，而且一般是需要付费才能提供给云用户的，或者是通过其他途径商业化的

社区云类似于公有云，只是它的访问被限制为特定的云用户社区，社区云可以是社区成员或提供具有访问限制的公有云的第三方提供者共同拥有的，社区的云用户成员通常会共同承担定义和发展社区云的责任

私有云是由一家组织单独拥有的，私有云使得组织把云计算技术当做一种手段，可以集合访问不同部分、位置或部门的 IT 资源

混合云是由两个或者更多云部署模型组成的云环境

第五章 云使能技术

与地理上分散的 IT 资源相比，彼此邻近成组的 IT 资源有利于能源共享、提供共享 IT 资源使用率以及提高 IT 人员的效率。现代数据中心是指一种特殊的 IT 基础设施，用于集中放置 IT 资源，包括服务器、数据库、网络与通信设备以及软件系统

虚拟化是将物理 IT 资源转换为虚拟 IT 资源的过程，大多数 IT 资源都能被虚拟化，包括服务器、存储设备、网络和电源

运行虚拟化软件的物理服务器称为主机或物理主机，其底层硬件可以被虚拟化软件访问。虚拟化软件功能包括系统服务，具体说来是与虚拟机管理相关的服务，这些服务通常不会出现在标准操作系统中，因此，这种软件有时也称为虚拟机管理器或虚拟机监视器，而最常见的

称呼为虚拟机监控器（hypervisor）
虚拟化软件提供的协调功能可以在一个虚拟主机上同时创建多个虚拟服务器，虚拟化技术允许不同的虚拟服务器共享同一个物理服务器，这就是服务器整合，通常用于提高硬件利用率、负载均衡以及对可用 IT 资源的优化。服务器整合带来了灵活性，使得不同的虚拟服务器可以在同一台主机上运行不同的客户操作系统

基于操作系统的虚拟化是指，在一个已存在的操作系统上安装虚拟化软件，这个已存在的操作系统被称为宿主操作系统

基于硬件的虚拟化是指将虚拟化软件之间安装在物理主机硬件上，从而绕过宿主操作系统，这也适用于基础操作系统的虚拟化，由于虚拟服务器与硬件的交互不再需要宿主操作系统的中间环节，因此，基于硬件的虚拟化通常更高效

虚拟化 IT 资源的管理通常是由虚拟化基础设施管理（VIM）工具予以实现

通常用来改进开销问题的策略是一种称为半虚拟化的技术，它向虚拟机提供了一个不同于底层硬件的软件接口

虚拟化和多租户的区别在于作为主机的物理服务器上多倍化的是什么
虚拟化：一个物理服务器上可以容纳服务器环境的多个虚拟副本，每个副本都可以提供给不同的用户，可以独立配置，还可以包含自己的操作系统和应用程序
多租户：要给物理或虚拟服务器运行着一个应用程序，该程序允许被多个不同用户共享，每个用户都感觉只有自己在使用该应用程序

服务代理是事件驱动程序，它在运行时拦截消息，服务代理分为主动服务代理和被动服务代理。主动服务代理在拦截并读取消息内容后，会采取一定措施，通常是修改消息的内容（最常见的是修改消息头部数据，少部分会要求修改消息体数据）或者修改消息路径。被动服务代理不会修改消息内容，而是在读取消息后，捕捉特定内容以便进行监控、记录或者报告

第六章 基本云安全
保密性是指事物只有被授权才能访问的特性，在云环境中，保密性主要是关于对传输和存储的数据进行访问限制的

完整性是指未被未授权方篡改的特性

真实性是指事物是经由授权的源提供的这一特性

可用性是在特定的时间段内可以访问和可以使用的特性

威胁是潜在的安全性违反，可能试图破坏隐私并/或导致危害，以此挑战防护。有手动或自动策动的威胁被设计用来利用已有的弱点，这些弱点称为漏洞，威胁实施的结果就是攻击

漏洞是一种可能被利用的弱点，可能是因为安全控制保护不够，也可能是因为攻击击败了现有的安全控制。造成 IT 资源漏洞的原因有很多，包括配置缺陷、安全策略弱点、用户错误、

硬件或者固件缺陷、软件漏洞和安全架构薄弱

风险是指执行一个行为带来损失或危害的可能性

安全控制是用来预防或响应安全威胁以及降低或避免风险的对策

安全策略建立了一套安全规则和规章，通常，安全策略会进一步定义该如何实现和加强这些规则和规章

威胁作用者是引发威胁的实体，因为它能够实施攻击，云安全威胁可能来自内部也可以来自外部，可能来自于人也可能来自于软件程序

匿名攻击者是云中没有权限的、不被信任的云服务用户，它通常是一个外部软件程序，通过公网发送网络攻击

恶意服务作用者能截取并转发云内的网络流量，它通常是带有被损害的或恶意逻辑的服务代理（或伪装成服务代理的程序），也有可能是能够远程截取并破坏消息内容的外部程序

授信的攻击者与同一云环境中的云用户共享 IT 资源，试图利用合法的证书来把云提供者以及与他们共享 IT 资源的云租户作为攻击目标

恶意的内部人员是人为的威胁作用者，他们的行为代表云提供者或者与之有关，这种类型的威胁作用者会带来极大的破坏可能性，因为恶意的内部人员可能拥有访问云用户 IT 资源的管理特权

流量窃听是指当数据在传输到云中或在云内部传输时（通常是从云用户到云提供者）被恶意的服务作用者被动地截获，用于非法的信息收集之目的。这种攻击的目的就是直接破坏数据的保密性，可能也破坏了云用户和云提供者之间关系的保密性。由于这种攻击被动的本质，这种攻击更容易长时间进行而不被发现

恶意媒介威胁是指消息被恶意服务作用者截获并且被篡改，因此可能会破坏消息的保密性和完整性，它还有可能在把消息转发到目的地之前插入有害的数据

拒绝服务攻击的目标是使 IT 资源过载至无法正确运行，这种形式的攻击通常是以以下方式之一发起的：
云服务上的负载由于伪造的消息或重复的通信请求不正常地增加
网络流量过载，降低了响应性，性能下降
发出多个云服务请求，每个请求都设计成消耗过量的内存和处理资源

授权不足攻击是指错误地授予了攻击者访问权限或是授权太宽泛，导致攻击者能够访问到本应该受到保护地 IT 资源，通常结果就是攻击者获得了对某些 IT 资源地直接访问的权利，这些 IT 资源实现的时候是假设只能是授信的用户程序才能访问的。这种攻击的一种变种称为弱认证，如果用弱密码或共享账户来保护 IT 资源，就可能导致这种攻击

虚拟化攻击利用的是虚拟化平台中的漏洞来危害虚拟化平台保密性、完整性和可用性。

如果云中的物理 IT 资源是由不同的云服务用户共享的，那么这些云服务用户的信任边界是重叠的，恶意的云服务用户可以把目标设定为共享的 IT 资源，意图损害其他共享同样信任边界的云服务用户或 IT 资源。结果是某些或者所有其他的云服务用户都受到攻击的影响，或者攻击者可能使用虚拟 IT 资源来攻击其他共享同样信任边界的用户

第七章 云基础设施机制

逻辑网络边界被定义为将一个网络环境与通信网络的其他部分分隔离开来，形成了一个虚拟网络边界，它包含并隔离了一组相关的基于云的 IT 资源，这些 IT 资源在物理上可能是分布式的，该机制可被用于：

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

逻辑网络边界通常由提供和控制数据中心连接的网络设备来建立，一般是作为虚拟化 IT 资源进行部署的，其中包括：

虚拟防火墙：一种 IT 资源，可以主动过滤被隔离网络的网络流量，并控制其与 Internet 的交互

虚拟网络：一般通过 VLAN 形成，这种 IT 资源用来隔离数据中心基础设施内的网络环境

虚拟服务器是一种模拟物理服务器的虚拟化软件，通过向云用户提供独立的虚拟服务器实例，云提供者使多个云用户共享同一个物理服务器

云使用监控机制是一种轻量级的自治软件程序，用于收集和处理 IT 资源的使用数据

云使用监控器可以以不同的形式存在，每种形式都将收集到的使用数据发送到日志数据库，以便进行后续处理和报告

监控代理是一个中间的事件驱动程序，它作为服务代理驻留在已有通信路径上，对数据流进行透明的监控和分析，这种类型的云使用监控通常被用来计算网络流量和消息指标

资源代理是一种处理模块，通过与专门的资源软件进行事件驱动的交互来收集使用数据，它在资源软件级上，监控预定义的且可观测事件的使用指标，比如：启动、暂停恢复和垂直扩展

轮询代理是一种处理模块，通过轮询 IT 资源来收集云服务使用数据，它通常被用于周期性地监控 IT 资源状态，比如正常运行时间与停机时间

复制被定义为对同一个 IT 资源创建多个实例，通常在需要加强 IT 资源的可用性和性能时执行，使用虚拟化技术来实现资源复制机制可以复制基于云的 IT 资源

已就绪环境机制是 PaaS 云交付模型的定义组件，它代表的是预定义的基于云的平台，该平台由一组已安装的 IT 资源组成，可以被云用户使用和定制。云用户使用这些环境在内远程

开发和配置自身的服务与应用程序。典型的已就绪环境包括预定义的 IT 资源，如数据库、中间件、开发工具和管理工具

第八章 特殊云机制

自动伸缩监听器机制是一个服务代理，它监控和追踪云服务用户和云服务之间的通信，用以动态自动伸缩。自动伸缩监听器部署在云中，通常靠近防火墙，在这里它们自动追踪负载状态信息。负载量可以由云用户产生的请求或某种类型的请求引发的后端处理需求量来决定。对于不同负载波动的条件，自动伸缩监听器可以提供不同类型的响应，例如：

根据云用户事先定义的参数，自动伸缩 IT 资源

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，采用这种方式，云用户能选择调节它当前的 IT 资源分配

水平扩展的常见方法是把负载在两个或更多的 IT 资源上做负载均衡，与单一 IT 资源相比，这提升了性能和容量。负载均衡器机制是一个运行时代理，其逻辑基本上就是基于这个思想的。除了简单的劳动分工算法，负载均衡器可以执行一组特殊的运行时负载分配功能，包括：

非对称分配：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：负载根据其优先等级进行调度、排队、丢弃和分配

上下文感知的分配：根据请求内容的指示把请求分配到不同的 IT 资源

SLA 监控器机制被用来专门观察云服务的运行时性能，确保它们履行了 SLA 中公布的约定 QoS 需求。SLA 监控器收集的数据由 SLA 管理系统处理并集成到 SLA 报告的标准中。当异常条件发生时，例如当 SLA 监控器报告有云服务“下线”时，系统可以主动地修复或故障转移云服务

按使用付费监控器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，并生成使用日志用于计算费用

审计监控器机制用来收集网络和 IT 资源的设计记录数据，用以满足管理需要或者合同义务。

故障转移系统机制通过使用现有的集群技术提供冗余的实现来增加 IT 资源的可靠性和可用性。故障转移系统会被配置成只要当前活动的 IT 资源变得不可用时，便自动切换到冗余的或待机 IT 资源实例上。故障转移系统有两种基本配置：主动-主动、主动-被动

在主动-主动配置中，IT 资源的冗余实现会主动地同步服务工作负载，在活动的实例之间进行负载均衡，当发现故障时，把失效的实例从负载均衡调度器中移除

在主动-被动配置中，待机或非活跃的实现会被激活，从变得不可用地 IT 资源处接管处理工作，相应的工作负载就会被重定向到接管操作的这个实例上

虚拟机监控器机制是虚拟化基础设施的最基础部分，主要用来在物理服务器上生成虚拟服务器实例。虚拟机监控器通常限于一台物理服务器，因此只能创建那台服务器的虚拟映像。类似地，虚拟机监控器只能把它自己创建的虚拟服务器分配到位于同一底层物理服务器上的资源池里

基于云的 IT 资源在地理上是分散地，但是逻辑上可以合并成组以改进它们的分配和使用。资源集群机制是把多个 IT 资源实例分为一组，使得它们能像一个 IT 资源那样进行操作，这

增强了集群化 IT 资源的组合计算能力、负载均衡能力和可用性
资源集群有两种基本类型：负载均衡的集群和 HA 集群
负载均衡集群地专长在于在集群节点中国分布工作负载，既提高 IT 资源的容量又保持 IT 资源的集中管理，它通常要实现一个负载均衡器机制，要么是嵌入集群管理平台，要么是设定为一个独立的 IT 资源
HA 集群：高可用集群在遇到多节点失效的情况下，仍然能够维持系统的可用性，而且大多数或者所有集群化的 IT 资源都有冗余实现。它实现一个故障转移系统机制，监控失效情况，并自动将工作负载重定向为远离故障节点

一个云服务可能会被大量云服务用户访问，而它们对主机硬件设备和通信需求都不同，为了克服云服务和迥异的云服务用户之间的不兼容性，需要创建映射逻辑来改变（或转换）运行时交换信息。多设备代理机制用来帮助运行时的数据交换，使得云服务能够被更广泛的云服务用户程序和设备所使用

状态管理数据库是一种存储设备，用来暂时地持久化软件程序地状态数据。作为把状态数据缓存在内存中地一种替代方法，软件程序可以把状态数据卸载到数据库中，用以降低程序占用地运行时内存。由此，软件程序和周边地基础设施都具有更大的可扩展性。状态管理数据库通常是由云服务使用的，特别是涉及长时间运行时活动的服务

远程管理系统机制向外部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。远程管理系统能够建立一个入口以便访问各种底层系统的控制与管理功能，这些功能包括资源管理、SLA 管理和计费管理

资源管理系统机制帮助协调 IT 资源，以便响应云用户和云提供者执行的管理操作。此系统的核心是虚拟基础设施管理器（VIM），它用于协调服务器硬件，这样就可以从最合适的底层物理服务器创建虚拟服务器实例。VIM 是一个商业化产品，它用于管理一系列跨多个物理服务器的 IT 资源

SLA 管理系统机制代表的是一系列商品化的可用云管理产品，这些产品提供的功能包括：SLA 数据的管理、收集、存储、报告以及运行时通知

计费管理系统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。具体来说，计费管理系统依靠按使用付费监控器来收集运行时使用数据。这些数据存储在系统组件的一个库中，然后为了计费、报告和开发票等目的，从库中提取数据

默认情况下，数据按照一种可读的格式进行编码，这种格式称为明文，当明文在网络上传输时，容易遭受未被授权的和潜在的恶意访问。加密机制是一种数字编码系统，专门用来报数数据的保密性和完整性，它用来把明文数据编码成为受保护的、不可读的格式
把原始的明文数据转换成加密的数据，称谓密文。当对明文进行加密时，数据与一个成为密钥的字符串结成对，其中密钥时由被授权的各方建立和共享的秘密消息，密钥用来把密文解密回原始的明文格式
加密机制可以帮助对抗流量窃听、恶意媒介、授权不足和信任边界重叠这样一些安全威胁
有两种常见的加密类型：对称加密和非对称加密
对称加密在加密和解密时使用的是相同的密钥，这两个过程都是由授权的各方用共享的密钥

执行的
非对称加密依赖于使用两个不同的密钥，称为私钥和公钥。在非对称加密（也被称为公钥密码技术）中，只有所有者才知道私钥，而公钥一般来说是可得的。一篇用某个私钥加密的文档只能用相应的公钥正确解密。相反地，以某个公钥加密的文档也只用与之对应的私钥解密。

当需要一种单向的、不可逆的数据保护形式时，就会使用哈希机制。对消息进行哈希时，消息就被锁住了，并且不提供密钥打开该消息，这种机制的常见应用时密码的存储。
除了用来保护存储数据外，可以用哈希机制减轻的云威胁包括恶意媒介和授权不足

数字签名机制是一种通过身份验证和不可否认性来提供数据真实性和完整性的手段。在发送之前，赋予消息一个数字签名，如果之后消息发生了未被授权的修改，那么这个数字签名就会变得非法。数字签名提供了一种证据，证明收到的消息与合法的发送者创建的那个消息是否是一样的。数字签名的创建中涉及哈希和非对称加密，它实际上是一个由私钥加密了的消息摘要被附加到原始消息中，接收者要验证签名的合法性，用相应的公钥来解密这个数字签名，得到消息摘要。也可以对原始的消息应用哈希机制来得到消息摘要。两个不同的处理得到相同的结果表明消息保持了其完整性

数字签名机制帮助缓解恶意媒介、授权不足和信任边界重叠等安全威胁

管理非对称密钥颁发的常用方法是基于公钥基础设施（PKI）机制的，它是一个由协议、数据格式、规则和实施组成的系统，使得大规模的系统能够安全地使用公钥密码技术。这个系统用来把公钥与相应地密钥所有者联系起来（称为公钥身份识别），同时还要能验证密钥的有效性。PKI 依赖数字证书，数字证书是带数字签名的数据结构，它与公钥一起来验证证书拥有者身份以及相关信息，例如有效期。数字证书通常是由第三方证书颁发机构数字签发的，PKI 机制主要用于防御不充分的授权威胁

身份与访问管理机制包括控制和追踪用户身份以及 IT 资源、环境、系统访问特权的必要组件和策略，主要用来对抗授权不足、拒绝服务攻击和信任边界重叠等威胁

跨越多个云服务为云服务用户传播认证和授权信息是件很难的事情，特别是如果在同一个运行时活动中需要调用大量的云服务或基于云的 IT 资源时。单一登录机制使得一个云服务用户能够被一个安全代理认证，这个安全代理建立起一个安全上下文，当云服务用户访问其他云服务或者基于云的 IT 资源时，这个上下文会被持久化，否则，云服务用户要在后续的每个请求都重新认证它自己

就像构建堤坝把卢狄和水隔离一样，在 IT 资源之间设置隔离能够增加对数据的保护。云资源的分割过程时这样一个过程：为不同的用户和组创建各自的物理和虚拟 IT 环境
基于云的资源分割过程创建了基于云的安全组机制，这是通过安全策略来决定的。网络被分成逻辑的基于云的安全组，形成逻辑网络边界，每个基于云的 IT 资源至少属于一个逻辑的基于云的安全组。这种机制可以被用来帮助对抗拒绝服务、授权不足和信任边界重叠等威胁，也与逻辑网络边界机制密切相关

虚拟服务器是从一个被称为虚拟服务器映像（或虚拟机映像）的模板配置创建出来的。强化是这样一个过程：把不必要的软件从系统中剥离出来，限制可能被攻击者利用的潜在漏洞。

去除冗余的程序、关闭不必要的服务器端口、关闭不使用的服务、内部根账户和宾客访问，这些都是强化的例子
强化的虚拟服务器映像是已经经过强化处理的虚拟服务实例创建的模板，这通常会得到一个比原始标准映像更加安全的虚拟服务器模板。强化的虚拟服务器映像能够帮助对抗拒绝服务、授权不足和信任边界重叠等威胁

第 11 章 基本云架构
通过增加一个或多个相同的 IT 资源可以进行 IT 资源水平扩展，而提供运行时逻辑的负载均衡器能够在可用 IT 资源上均匀分配工作负载。由此产生的负载分布架构在一定程度上依靠复杂的负载均衡器算法和运行时逻辑，减少 IT 资源的过度使用和使用率不足的情况

资源池架构以使用一个或多个资源池为基础，其中相同的 IT 资源由一个系统进行分组和维护，以自动确保它们保持同步

动态可扩展架构是一个架构模型，它基于预先定义扩展条件的系统，触发这些条件会导致从资源池中动态分配 IT 资源。由于不需要人工交互就可以 有效地回收不必要地 IT 资源，所以，动态分配使得资源的使用可以按照使用需求的变化而变化

弹性资源容量架构主要与虚拟服务器的动态供给相关，利用分配和回收 CPU 与 RAM 资源的系统，立即响应托管 IT 资源的处理请求变化

服务负载均衡架构可以被认为是工作负载分布架构的一个特殊变种，它是专门针对扩展云服务实现的。在动态分布工作负载上增加负载均衡系统，就创建了云服务的冗余部署

云爆发架构建立了一种动态扩展的形式，只要达到预先设置的容量阈值，就从企业内部的 IT 资源扩展或“爆发”到云中。相应的基于云的 IT 资源是冗余性预部署，它们保持非活跃状态，直到发生云爆发。当不再需要这些资源后，基于云的 IT 资源被释放，而架构则“爆发入”企业内部，回到企业内部环境

通常对使用基于云的存储空间的云用户按照固定磁盘存储分配来收费，这就意味着费用已经按照磁盘容量预先定义好了，而与实际使用的数据存储量没有关系。弹性磁盘供给架构建立了一个动态存储供给系统，它确保按照云用户实际使用的存储量进行精确计费。该系统采用自动精简供给技术实现存储空间的自动分配，并进一步支持运行时使用监控来收集准确的使用数据以便计费。

云存储设备有时会遇到一些故障和破坏，造成这种情况的原因包括：网络连接问题、控制器或一般硬件故障或者安全漏洞。一个组合的云存储设备的可靠性会存在连锁反应，这会使云中依赖其可用性的全部服务、应用程序和基础设施组件都遭受故障影响。冗余存储架构引入了复制的辅云存储设备作为故障系统的一部分，它要与主云存储设备中的数据保持同步

第 12 章 高级云架构
虚拟机监控器可以负责创建和管理国歌虚拟服务器。因为这种依赖关系，任何影响虚拟机监控器失效的状况都会波及它管理的虚拟服务器。虚拟机监控器集群架构建立了一个跨多个物

理服务器的高可用虚拟机监控器集群。如果一个给定的虚拟机监控器或其底层物理服务器变得不可用，则被其托管的虚拟机服务器可迁移到另一物理服务器或虚拟机监控器上来保持运行时操作

在物理服务器之间保持跨服务器的工作负载均衡是很难的一件事情，因为物理服务器的运行和管理是相互隔离的，很容易就会造成一个物理服务器比它的邻近服务器承载过多的虚拟服务器或收到更高的工作负载。随着时间的变化，物理服务器的过低或过高使用都可能会显著增加，这导致持续的性能挑战（对过度使用的服务器）或持续的浪费（对使用过低的服务器，失去了处理的潜能）
负载均衡的虚拟服务器实例架构建立了一个容量看门狗系统，在把处理任务分配到可用 的物理服务器主机之前，会动态地计算虚拟服务器实例及其相关地工作负载

不中断服务重定位架构
造成云服务不可用的原因有：
运行时使用需求超出了它的处理能力
维护更新要求必须暂时中断
永久地迁移至新的物理服务器主机
如果一个云服务变得不可用，云服务用户的请求通常会被拒绝，这样有可能会导致异常的情况，即使中断是计划中的，也不希望发生云服务对云用户暂时不可用的情况
不中断服务重定位架构是这样一个系统：通过这个系统，预先定义的事件触发云服务实现的运行时复制或迁移，因而避免了中断。通过在新主机上增加一个复制的实现，云服务的活动在运行时可被暂时转移到另一个承载环境上，而不是利用冗余实现对云服务进行伸缩。类似地，当原始的实现因维护需要中断时，云服务用户的请求也可以被暂时重定向到一个复制的实现。云服务实现和任何云服务活动的重定位也可以是把云服务迁移到新的物理主机上

物理服务器自然地就是它承载地虚拟服务器地单一失效点，所以，当物理服务器故障或者被损害的时候，它承载的某些（或者所有）虚拟服务器都会受到影响，这使得云提供者向云用户做出的零宕（dang）机时间的承诺变得非常难保证
零宕机架构是一个非常复杂的故障转移系统，在虚拟服务器原始的物理服务器主机失效时，允许它们动态地迁移到其他物理服务器主机上

云负载均衡功能主要建立在自动伸缩监听器和故障转移系统机制结合地基础上

资源预留架构建立了一个系统，专门为给定的云用户保留下述的某种资源：单个 IT 资源、一个 IT 资源的一部分、多个 IT 资源。这就避免了资源受限和资源借用情况，从而使云用户免受互相的影响

动态故障检测和恢复架构建立起了一个弹性的看门狗系统，以监控范围广泛的预先定义的故障场景，并对之作出响应。对于自己不能自动解决的故障情况，该系统会发出通知，并作升级处理。它依赖于一个特殊的云使用监控器，称为智能看门狗监控器，主动地追踪 IT 资源，对预先定义的事件采取预先定义的措施

所谓裸机服务器是指没有预装操作系统或其他任何软件的物理服务器。裸机供给架构建立起的系统利用了这个特性以及特殊的服务代理，后者用来发现并有效地远程提供整个操作系统

快速供给架构建立的系统将大范围的IT资源供给进行了自动化，这些IT资源可以是单个的，也可以是联合起来的。存储负载管理架构使得 LUN（逻辑单元号）可以均匀地分布在可用地云存储设备上，而存储容量系统则用来确保运行时工作负载均匀地分布在 LUN 上

通过基于虚拟机监控器的处理层向托管的虚拟服务器提供对安装在物理服务器上的物理 I/O 的访问，被称为 I/O 虚拟化。使用直接 I/O 访问架构，允许虚拟服务器绕过虚拟监控器直接访问物理服务器的 I/O 卡，而不用通过虚拟机监控器进行仿真连接

直接 LUN 访问架构通过物理 HBA 卡向虚拟服务器提供了 LUN 访问。由于同一集群中的虚拟服务器可以将 LUN 当作集群数据库的共享卷来使用，因此，这种架构是有效的

动态数据规范化架构建立了一个重复删除系统，它通过侦测和消除云存储设备上的冗余数据来阻止云用户无意识地保留冗余的数据副本。这个系统既可以用于基于块的存储设备，也可以用于基于文件的存储设备，但前者最有效。当重复删除系统接收到一个数据块，就会将其与收到的块进行比较，以判断收到的块是否为冗余。冗余块会由指向存储设备中已有的相同块的指针来代替

弹性网络容量架构建立了一个系统，用于给网络动态分配额外带宽，以避免运行时出现瓶颈，该系统确保每个云用户使用不同的网络端口来隔离不同云用户的数据流量

跨存储设备垂直分层架构建立了一个系统，通过在容量不同的存储设备之间垂直扩展，使得该系统能够不受带宽和数据处理能力的限制。LUN 能在这个系统中的多个设备间自动进行向上向下扩展，因此，通过请求就可以使用合适的存储设备来执行云用户的任务

存储设备内部垂直数据分层架构建立了支持在单个云存储设备中进行垂直扩展的系统，这种设备内部的扩展优化了不同容量的各类磁盘的可用性

负载均衡的虚拟交换机架构建立了一个负载均衡系统，提供了多条上行链路来平衡多条上行链路或冗余路径之间的网络流量负载，从而有助于避免出现传输迟缓和数据丢失。执行链路聚合可以平衡流量，它使得工作负载同时分布在多个上行链路中，因此，不会有网卡出现超负荷的情况

多路径资源访问架构建立了一个多路径系统，它为 IT 资源提供可替换的路径。因此，云用户可以通过变成或手动方式克服路径故障

在持久虚拟网络配置架构中，网络配置信息进行集中存储，并复制到所有的物理服务器主机上，这使得一个虚拟服务器从一个主机移动到另一个主机时，目的主机可以访问配置信息

虚拟服务器的冗余物理连接架构建立一条或多条冗余上行链路连接，并将它们置为备用模式，一旦主上行链路连接变得不可用，该架构确保有冗余上行链路可以连接到有效的上行链路

需要进行停机维护的云存储设备上的数据可以暂时移到复制的辅助云存储设备上，存储维护

窗口架构自动且透明地将云服务用户重定位到辅云存储设备上，这些用户不会感知到其主存储设备已经停机下线

1、 系统虚拟化技术

硬件仿真（Emulation）

简介：属于 Hosted 模式，在物理机的操作系统上创建一个模拟硬件的程序（Hardware VM）来仿真所想要的硬件，并在此程序上跑虚拟机，而且虚拟机内部的客户操作系统（Guest OS）无需修改。知名的产品有 Bochs，QEMU 和微软的 Virtual PC（它还使用少量的全虚拟化技术）。

优点：Guest OS 无需修改，而且非常适合用于操作系统开发，也利于进行固件和硬件的协作开发。固件开发人员可以使用目标硬件 VM 在仿真环境中对自己的实际代码进行验证，而不需要等到硬件实际可用的时候。

缺点：速度非常慢，有时速度比物理情况慢 100 倍以上。

未来：因为速度的问题，渐趋颓势，但是还应该有一席之地。

全虚拟化（Full Virtulization）

简介：主要是在客户操作系统和硬件之间捕捉和处理那些对虚拟化敏感的特权指令，使客户操作系统无需修改就能运行，速度会根据不同的实现而不同，但大致能满足用户的需求。这种方式是业界现今最成熟和最常见的，而且属于 Hosted 模式和 Hypervisor 模式的都有，知名的产品有 IBM CP/CMS，VirtualBox，KVM，VMware Workstation 和 VMware ESX（它在其 4.0 版，被改名为 VMware vSphere）。

优点：Guest OS 无需修改，速度和功能都非常不错，更重要的是使用非常简单，不论是 VMware 的产品，还是 Sun（Oracle？）的 VirtualBox。

缺点：基于 Hosted 模式的全虚拟产品性能方面不是特别优异，特别是 I/O 方面。

未来：因为使用这种模式，不仅 Guest OS 免于修改，而且将通过引入硬件辅助虚拟化技术来提高其性能，我个人判断，在未来全虚拟化还是主流。

半虚拟化（Parairtulization）

简介：它与完全虚拟化有一些类似，它也利用 Hypervisor 来实现对底层硬件的共享访问，但是由于在 Hypervisor 上面运行的 Guest OS 已经集成与半虚拟化有关的代码，使得 Guest OS 能够非常好地配合 Hyperivosr 来实现虚拟化。通过这种方法将无需重新编译或捕获特权指令，使其性能非常接近物理机，其最经典的产品就是 Xen，而且因为微软的 Hyper-V 所采用技术和 Xen 类似，所以也可以把 Hyper-V 归属于半虚拟化。

优点：这种模式和全虚拟化相比，架构更精简，而且在整体速度上有一定的优势。

缺点：需要对 Guest OS 进行修改，所以在用户体验方面比较麻烦。

未来：我觉得其将来应该和现在的情况比较类似，在公有云（比如 Amazon EC2）平台上应该继续占有一席之地，但是很难在其他方面和类似 VMware vSphere 这样的全虚拟化产品竞争，同时它也将会利用硬件辅助虚拟化技术来提高速度，并简化架构。

硬件辅助虚拟化（Hardware Assisted Virtualization）

简介：Intel/AMD 等硬件厂商通过对部分全虚拟化和半虚拟化使用到的软件技术进行硬件化（具体将在下文详述）来提高性能。硬件辅助虚拟化技术常用于优化全虚拟化和半虚拟化产品，而不是独创一派，最出名的例子莫过于 VMware Workstation，它虽然属于全虚拟化，但是在它的 6.0 版本中引入了硬件辅助虚拟化技术，比如 Intel 的 VT-x 和 AMD 的

AMD-V。现在市面上的主流全虚拟化和半虚拟化产品都支持硬件辅助虚拟化，包括 VirtualBox，KVM，VMware ESX 和 Xen。
优点：通过引入硬件技术，将使虚拟化技术更接近物理机的速度。
缺点：现有的硬件实现不够优化，还有进一步提高的空间。
未来：因为通过使用硬件技术不仅能提高速度，而且能简化虚拟化技术的架构，所以预见硬件技术将会被大多数虚拟化产品所采用。

操作系统级虚拟化（Operating System Level Virtualization）
简介：这种技术通过对服务器操作系统进行简单地隔离来实现虚拟化，主要用于 VPS。主要的技术有 Parallels Virtuozzo Containers，Unix-like 系统上的 chroot 和 Solaris 上的 Zone 等。
优点：因为它是对操作系统进行直接的修改，所以实现成本低而且性能不错。
缺点：在资源隔离方面表现不佳，而且对 Guest OS 的型号和版本有限定。
未来：不明朗，我觉得除非有革命性技术诞生，否则还应该属于小众，比如 VPS。