

第四章答案

1. 分析讨论云的几个特性。

- 1) 按需使用：云用户不需要拥有 IT 资源，而是以服务的形式，需要的时候可以使用资源，不需要的时候就停止使用。
- 2) 泛在接入：一个云服务可以被广泛访问的能力。拥有 I 基础资源的云服务提供者可以通过网络线路来让大范围云用户访问到云资源，只要云用户与 IT 资源有线路链接。
- 3) 多租户：多租户是指不同的租户（团体/机构）可以共享应用软件，这些应用部署在云端。通过多租户，云服务供应商可以通过相同的应用程序为不同的租户（组织、团体）的用户提供服务。多租户可以减少软件版本，降低软件开发、维护成本。
- 4) 弹性：弹性即是能够根据用户的需求自动的扩展提供给用户的资源。与上面的按需使用不同，按需使用是体现在用户层面的，而弹性则是体现在云服务提供者层面的。
- 5) 可测量的使用：云平台对云用户使用的 IT 资源使用情况的记录能力，方便对用户进行收费，并且还可用于对 IT 资源的监控。
- 6) 可恢复性计算：是一种故障转移的形式。会在多个物理位置提供冗余的 IT 资源，并存放 IT 资源的备份。当前使用的 IT 资源出现故障的时候，就可以快速转换到备份资源进行处理，增加云服务的可靠性和可用性。

2. 分析讨论云计算中 4 个基本角色和他们之间的关系。

- 1) 云提供者：是指拥有云中的 IT 资源的实体。云提供者需要购置、部署、运维 IT 资源，包括计算、网络、软件等各类资源。这些资源可以以物理资源或者虚拟资源的形式提供给云用户。
- 2) 云用户：组织机构（或者个人），他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。
- 3) 云服务拥有者：在法律上部署和拥有云服务的个人或者组织称为云服务拥有者。可以是云用户，或者是拥有该云服务所在的云的云提供者。
- 4) 云资源管理者：负责管理基于云的 IT 资源的人或者组织。可以是云服务所属云的云用户或者云提供者，也可以是签订了合约来管理基于云的 IT 资源的第三方组织。

3. 分析讨论三种基本的交付模型中云用户的控制程度。

- 1) 基础设施作为服务（IaaS）：赋予用户完全的管理权限，可用的功能类型包括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，
- 2) 平台作为服务（PaaS）：赋予云用户有限的管理权限，可用的典型功能有对于云用户使用平台相关的 IT 资源的中等级别的管理控制。
- 3) 软件作为服务（SaaS）：赋予云用户的控制等级为使用和与使用相关的配置，云用户可以使用前端用户接口访问。

第五章答案

1. 以某个具体特权指令为例，针对某种具体的 CPU 虚拟化技术，描述其执行过程，并据此分析虚拟化技术的特点。

答：开放性问题

以 x86 架构的敏感指令 POPF 和全虚拟化技术为例。采用优先级压缩技术使 Guest OS 和 VMM 分别运行在 Ring 1 和 Ring 0 特权下，当 Guest OS 调用特权指令时，就自动陷入到 VMM 中，由 VMM 模拟执行。但 POPF 作为 x86 架构中的非特权敏感指令，在执行时无法

自动被 VMM 捕获，因此需要利用二进制代码翻译技术将其转化为支持虚拟化的指令，再由 VMM 实现从栈顶弹出一个字到模拟 CPU 的 EFLAGS 中的操作。可以看出，在虚拟化技术中 VMM 通过控制 Guest OS 的敏感指令实现了对物理硬件的全面接管，但同时又保证了虚拟机的执行与物理机执行的等效性。

虚拟化技术特点：

- 1) 分区：大型的、扩展能力强的硬件能够被用来作为多台独立的服务器使用； 在一个单独的物理系统上，可以运行多个操作系统和应用； 计算资源可以被放置在资源池中，并能够被有效地控制。
- 2) 隔离：虚拟化能够提供理想化的物理机，每个虚拟机互相隔离； 数据不会在虚拟机之间泄露； 应用只能在配置好的网络连接上进行通讯。
- 3) 封装：虚拟单元的所有环境被存放在一个单独文件中； 为应用展现的是标准化的虚拟硬件，确保兼容性； 整个磁盘分区被存储为一个文件，易于备份、转移和拷贝。
- 4) 硬件独立：可以在其他服务器上不加修改的运行虚拟机。虚拟技术支持高可用性、动态资源调整，极大地提高系统的可持续运行能力。

2 . 讨论分析 MapReduce 计算模式与一般的分布式计算、并行计算的异同。

答到具体特点即可。

相同点：把一个大问题分解成许多子问题，利用多个计算节点/CPU 核心分别进行处理，以缩短解决整个问题的时间。

异：并行计算是相对于串行计算而言的，它通常关注单个节点上的多个 CPU 核心之间的并行协作，而不是节点间的通信。MapReduce 和分布式计算通常将任务分发到网络中的多个节点，分别处理后再汇总结果。MapReduce 对一次计算过程的 Map 和 Reduce 阶段做了明显的定义和区分，而一般的分布式计算根据任务的不同有可能具有其他形式的阶段性特征。

3 . 讨论分析微服务技术对云计算的弹性、高可用性等特性的支撑作用。

1) 微服务技术对云计算的弹性的支撑作用：云计算的弹性是一种能力，是指云根据运行时条件或云用户或云提供者事先确定的要求，自动透明地拓展 IT 资源。使用微服务架构，可以将每种服务对应的各个小逻辑和其所需的数据封装起来，这样封装之后每个小的服务模块都可以独立部署和运行，因此可以弹性地扩展每一个小模块，同时还可以弹性组合各个模块的功能，由此说明了微服务技术对云计算的弹性的支撑作用。

2) 微服务技术对云计算的高可用性的支撑作用：高可用性通常来描述一个系统经过专门的设计，从而减少停工时间，而保持其服务的高度可用性。在微服务技术中，每一个微服务都会部署多个服务实例来为客户端提供服务，保证了服务高可用，说明了微服务技术对云计算的高可用性的支撑作用。

第 6 章答案

1.分析讨论几个不同的威胁作用者

1) 匿名攻击者

匿名攻击者(Anonymous Attacker)是云中没有限权的、不被信任的云服务用户

2) 恶意服务作用者

恶意服务作用者(Malicious Service Agent)能截取并转发云内的网络流量

3) 授信的攻击者

授信的攻击者(Trusted Attacker)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他们共享 IT 资源的云租户作为攻击目标

4) 恶意的内部人员

恶意的内部人员(Malicious Insider)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

2. 分析讨论云安全威胁中常见威胁的引发原因和目的

1) 流量窃听

流量窃听(Traffic Eavesdropping)是指但数据在传输到云中或在云内部传输时被恶意的服务作用者被动地截获，用于非法的信息收集的目的。

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。

由于这种攻击被动地本质，这种攻击很容易被长时间忽略。

2) 恶意媒介

恶意媒介(Malicious Intermediary)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。

它还可能在把消息转发到目的地之前注入有害的数据。

一个恶意云用户程序可能带来恶意媒介攻击。

3) 拒绝服务

拒绝服务(Denial of Service)攻击的目标是使 IT 资源过载至无法正确运行。

通常是以下方式之一发起的：

(1)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。

(2)网络流量过载，降低了响应性，性能下降。

(3)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。

成功的 DoS 攻击使得服务器性能恶化或失效。

4) 授权不足

授权不足(Insufficient Authorization)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保护的 IT 资源。

授权不足的结果通常是攻击者获得了对某些 IT 资源的直接访问的权利，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。

5) 虚拟化攻击

虚拟化攻击是指云提供者给予用户的虚拟化 IT 资源的管理权限，用户滥用权限攻击底层的物理资源。

目的是危害虚拟化平台的保密性、完整性和可用性。

6) 信任边界重叠

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(Overlapping Trust Boundaries)。

恶意的云服务用户可以把目标设定为共享的 IT 资源，意图损害其他贡献同样信任边界的云服务用户或 IT 资源。

第 7 章答案

1、说说你对虚拟服务器的理解，以及这种机制的作用。

虚拟服务器是一种模拟物理服务器的虚拟化软件。

虚拟服务器是最基本的云环境构建块。

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。

通过安装或释放虚拟服务器，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。

2、分析讨论每个云存储等级以及对应的云存储设备和相关联的技术接口。

文件（file）——存放于文件夹中

块（block）——存储的最低等级，最接近硬件，可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

网络存储接口——文件或块

对象存储接口——Web 资源

数据库存储接口——分为关系数据存储和非关系数据存储（NoSQL）

3、分析讨论云使用监控的 3 种实现形式。

监控代理是一个中间的时间驱动程序，对数据流进行透明的监控和分析。（见 Figure7.12）

资源代理是一种处理模块，在资源软件级别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。（见 Figure7.13）

轮询代理是一种处理模块，通过轮询 IT 资源来周期性地监控 IT 资源状态（比如正常运行时间和停机时间）。（见 Figure7.14）

第 8 章答案

1. 讨论分析可以用于自动伸缩的判定条件和机制。

自动伸缩是一个通过监控和追踪云服务用户和云服务之间的通信情况，分析 IT 资源使用，并采取相应行动的机制

- 1、自动伸缩判定条件：负载量，具体大致是两种 1) 云用户产生的请求量；2) 某种类型的请求引发的后端处理需求量
- 2、自动伸缩的机制：1) 自动伸缩，根据云用户预定义的参数值，监听器自动地进行 IT 资源的分配；2) 被动通知，监听器监听负载是否超过或者少于某个阈值，然后通知用户，由用户来决定是否要增加或减少 IT 资源的分配。

2. 分析讨论按使用付费监控器的两种实现方式的优缺点。

1) 监控代理：

监控代理是通过在整个服务端的入口监控用户的请求来间接地判断用户使用云服务的情况。

优点：只需在云集群的入口部署，使用维护方便。

缺点：因为不是直接对实际情况检测，所以监测的值可能不够准确。

2) 资源代理：

资源代理需要在部署在各个资源前，实时地轮询每一个资源的使用情况。

优点：针对每一种资源进行实时的监测，能够及时正确的反映资源的使用情况。

缺点：因为需要对每一个资源进行监测，所以需要的监控代理数量会比较多，维护麻烦。

第 9 章答案

1、云资源管理者可以通过哪些方式对云中的 IT 资源进行管理？分析讨论各自的优缺点。

答：可以从两个角度来讲。

- 1) 通过不同的管理系统来对 IT 资源进行管理：远程管理系统，资源管理系统，SLA 管理系

统，计费管理系统。

2) 外部访问（远程访问）使用与管理入口，本地 VIM 控制台进行管理。

然后再讨论各自的优缺点。

PS：写出方式得 3 分，加上分析优缺点得 5 分。

IT 资源管理方式	优点	缺点
远程管理系统	向外部云资源管理者提供工具和用户界面	受网络质量影响
资源管理系统	协调 IT 资源，响应管理操作；从最合适的底层服务器创建虚拟服务器实例	虚拟资源迁移可能产生性能上的损失
SLA 管理系统	按服务质量收费，保障服务有效性	难以确定服务崩溃原因
计费管理系统	按使用付费，允许指定不同的定价规则	没有考虑服务质量

或：（亦可额外补充优缺点）

IT 资源管理方式	优点	缺点
外部访问	不受物理位置限制，可远程访问	受网络质量影响
本地 VIM 控制台	不受网络质量影响	受地理位置限制

2、SLA 管理系统与计费管理系统在操作步骤上有哪些主要不同之处？

答：

	SLA 管理系统	计费管理系统
使用的监控器不同	SLA 监控代理	按使用付费监控代理
存放的库不同	服务质量测量库	按使用付费计量库
使用的管理器不同	SLA 管理器	定价与合同管理器
生成内容不同	报告	发票

1) 使用的监控器不同：SLA 监控代理；按使用付费监控代理

注：或者说收集的数据不同

2) 存放的库不同：服务质量测量库；按使用付费计量库

3) 使用的管理器不同：SLA 管理器；定价与合同管理器

注：2) 和 3) 可以合并为 使用的管理系统不同：SLA 管理系统；计费管理系统

4) 生成内容不同：报告；发票

PS：将两个系统的步骤分别罗列出来的也算对，得 4 分；按以上回答的得 5 分

第 11 章答案

1、讨论分析负载均衡与动态扩展架构（水平扩展、弹性容量、弹性磁盘）之间的关联性。

答：

1) 可从不同的方面进行作答，以下（但不仅限于此）分别举例。

讨论负载均衡与动态扩展在概念和操作上的异同，直接使用书本上的概念或使用自己的语言组织。如：二者都是根据用户需求对 IT 资源进行分配。而负载均衡是静态资源分配，并且

目的是使服务负载均衡分布；动态扩展则是动态分配资源，根据用户需求的变化而自动扩展或回收资源。

2) 从水平扩展、弹性容量、弹性磁盘三个方面分别说明二者异同点。

2、调研不同的请求调度方法，并详细描述其中的一种。

答：开放性问题。

轮循，加权轮询，源 IP 哈希，加权最少连接数，基于代理的自适应负载均衡，加权响应等。