云计算基础与应用

南通师范高等专科学校
Nantong Normal College

朱亚林

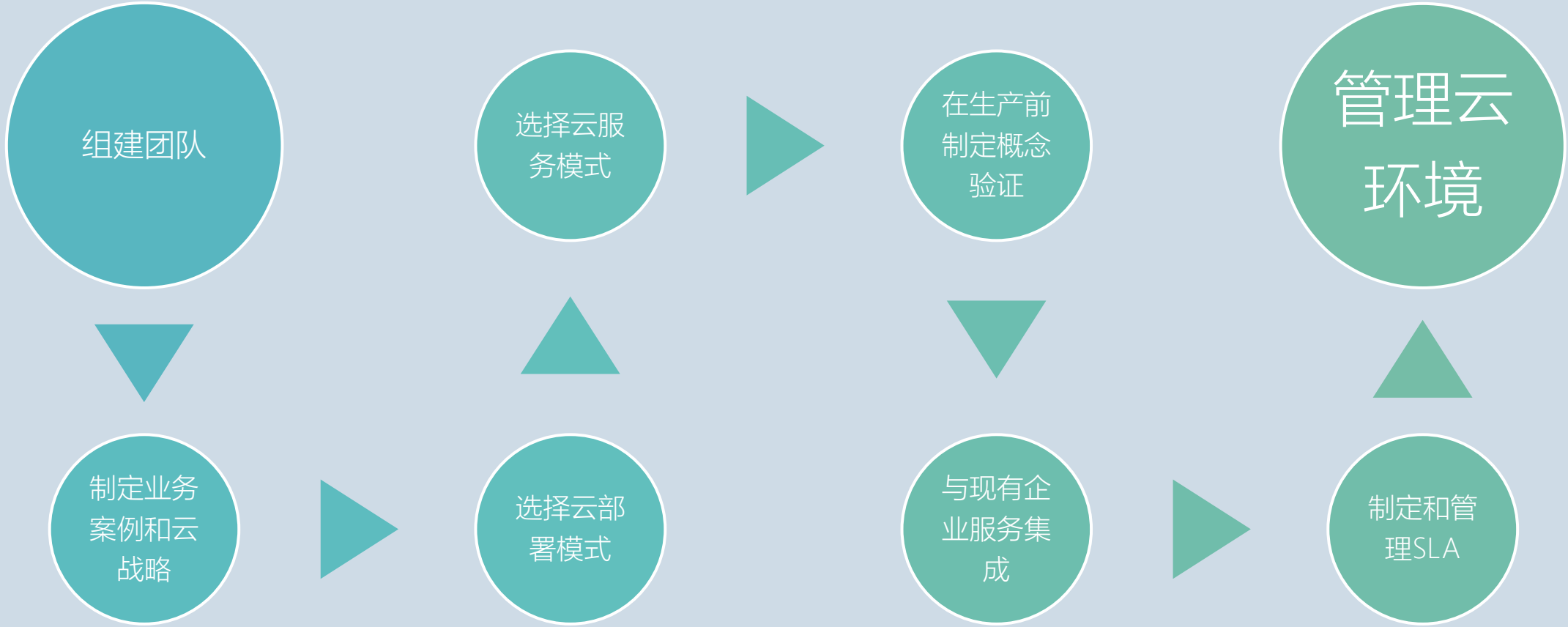
云计算架构及标准化

3.3 如何实施云计算

当前云计算关注的重点

- 探索和建立适宜云计算发展的市场准入、服务采购和安全保障机制，推广应用安全可靠的云产品和云解决方案，以及如何实施云计算，如何从用户的视角选择合适的云相关产品；
- 从应用的角度出发，服务水平协议（service level agreement,SLA）、云安全也是云计算在实施过程中云用户应关注的重点。

3.3.1 云计算实施总路线



1.组建团队

- 云用户可能是各类不同规模的企业，在决定采用云计算为自己服务时，需要建立相应的工作团队，并明确在云实施不同阶段时各角色的工作职责和工作目标。
- 在云服务的部署阶段，CEO和高级管理人员领导公司确定目标、职责范围和指导方针。在策略阶段，通常在CIO或CTO的领导下，公司执行业务分析和技术分析。在运营阶段，不同运营组的主管针对云部署，共同完成持续运营业务的采购、实施和运营。

2.制定业务案例和云战略

- 云用户应明确自身需求，结合自身业务特点，制定适合自身发展的综合云战略。在规划云战略时，应将以下工作考虑在内：培训团队、考虑现有IT环境、了解所需要的服务和功能、确定所需要的技能、制定长期和短期规划、确定明确的目标和衡量进度的指标、了解法律法规要求、延长追踪结果的时间。

3.选择云部署模式

根据既定云战略，综合考量企业规模、云服务关键程度、业务迁移成本、弹性、安全和多租户等因素，选择合适的云部署模式。

4.选择云服务模式

- 根据云用户的IT成熟度和企业规模，结合各类云服务模式的特点，选择适合用户需求的云服务模式（IaaS、PaaS、SaaS）。云用户应从技能、初始考虑项、服务更新，以及测试和部署这几个方面综合考虑选择哪类部署方式，也可以根据具体的云服务需求，同时利用多个方式。

5.在生产之前制定概念验证

- 一旦明确要实施云，可建立概念验证(POC)团队。假设POC成功，符合或超出预期，则云服务可以交付进行生产实施。POC既可以在公司内部实施，又可以直接在公有云中实施。POC和目标云环境之间可能存在的差异在生产环境迁移时，需要处理目标云环境。一旦完成全部测试，并且运行正常，就可进一步完善商务合同 、SLA等，将新的云服务投入生产。

6.与现有企业服务集成

- 有多种方法可以在云服务和现有服务之间建立无缝连接。若企业已确定采用开放基础设施标准，则云服务应建立在已实施的内容的基础上，可通过标准化的应用程序编程接口（API）来对此进行管理，这些API将成为云服务所支持的开放标准和企业现有服务之间的连接导管，实现云服务和企业服务之间的互操作性。
- 若企业没有确定要采用开放基础设施标准，则可使用新的云服务来设置基线。一个清晰的采用开放标准的计划能确保云服务的互操作性和可移植性，并简化新服务的基础流程，使之不受新的云服务的获取位置和方式的限制。

7.制定和管理SLA

- SLA是用于解决服务交付争议的书面协议。花费时间制定一份全面的SLA将有助于消除用户与提供商之间的预期异议,也有助于确保交付满意的服务水平。
- 在制定云用户(买方)和云供应商(卖方)之间的SLA时,不仅要考虑到不同类型的服务模式有不同的需求,还应关注的因素有组建内部SLA团队、为合约服务制定SLA、与供应商共同定义关键流程、定期与企业内的关键利益相关者举行评审会、定期与云供应商召开检查点会议等。

8.管理云环境

- 企业管理和运营云环境需要企业信息化主管与用户支持经理共同负责，前者整体负责，后者负责管理日常运营，并建立通畅的沟通渠道，如问题不能解决，须参考SLA中的相关规定。技术支持和用户支持因服务模式、部署模式与托管选择不同而异。若选择私有云，则对其的管理应与企业现有服务的管理一致。若选择私有云和公有云，则应在SLA中规定对其的管理责任。SLA要确定相关流程用以发现问题，确定负责人和问题影响范围，寻找可以用于解决问题的资源 。

3.3.2云SLA实施步骤

- 理解角色和责任
- 评估业务水平策略
- 了解各种服务模型和部署模型的区别
- 确定关键性能目标
- 评估安全和隐私保护要求
- 明确服务管理要求
- 为服务故障管理做准备
- 了解灾难恢复计划
- 建立有效的管理流程
- 了解退出流程

1.理解角色和责任

- 为使用户理解云SLA明示或暗示的具体角色和责任，必须了解云计算环境可能涉及的不同角色。一般包含以下5种云角色。

云用户：与云供应商维持业务关系或使用云供应商服务的个人或机构。

云供应商：有责任向云用户提供服务的个人、机构或实体。

云运营商：提供云供应商与云用户间云服务连接和传输的中介机构。

云代理商：管理云服务使用、表现和交付，并协调云供应商和云用户关系的机构。

云审计者：独立评估云服务、信息系统运营、云实施的性能和安全性的一方。

1.理解角色和责任

- 用户需要了解每种云角色在云环境交付中的活动与责任，为每种角色准确设定要求与服务水平。SLA对不同的角色有不同要求，不限于定量方面，也包含遵照标准和数据保护等定性要求。通过SLA实施步骤，每个步骤都将详细介绍用户与供应商在业务水平目标和服务水平目标方面应负的责任。

2.评估业务水平策略

- 由于SLA所述策略与业务策略相关，用户在评审云SLA时必须考虑关键的策略问题。SLA内描述的云供应商的数据策略可能是最关键的业务水平策略，需要对其进行仔细评估。
- SLA中涉及的数据策略包括数据保存、数据冗余、数据位置、新数据位置的研究、数据获取和数据隐私。
- 除了数据策略外，云SLA内所述的其他业务水平策略也需要仔细评估，这些业务水平策略包括承诺、可接受的使用策略、未涵盖服务列表、超额使用激活、支付与惩罚模式、治理/版本控制、续约、转让、支持、计划内维护、分包服务、许可软件和行业特定标准等。

3.了解各种服务模型和部署模型的区别

云供应商提供的服务一般都可归纳为3种主要的服务模型:IaaS、PaaS和SaaS。对每一种类型来说,云SLA内可能包含的云资源抽象水平、服务水平目标和关键性能指标各不相同。

除了服务模型外,云SLA还应包含服务部署条款,这些条款应确认部署模型、所采用的部署技术。

4.确定关键性能目标

云计算环境中的性能目标与服务交付的效率和准确性直接相关。性能一般通过可用性、响应时间事务处理率和处理速度来衡量,但很多其他因素也可以衡量性能和系统的质量。因此,用户必须确定哪些因素对其云环境最为重要,并确保SLA中包含这些因素。

对云用户非常重要的性能声明需要具备可测量性,可以由用户对其审计,并且书面记录在SLA中,从而满足协议双方对服务水平的要求。性能的考虑因素因支持的服务模型(IaaS、PaaS和SaaS)和各种模型提供的服务类型的不同而异,如IaaS模型提供网络存储和计算服务。

为了确保性能目标有意义，当透明性和一致性对加强云服务的可信赖性非常重要时,度量是一个关键考虑事项。度量时,一定要清楚指标是怎样使用的,从这些指标中能得到什么结论,不断对性能进行评估，使其达到具体的目标。

5.评估安全和隐私保护要求

确保云足够安全的首要措施是根据企业数据的重要性和敏感性创建分类方案,在整个企业内部履行。该方案应包括数据所有权、对安全水平的合适定义和保护控制等方面的详细信息,以及对数据保留与删除需求的简单描述。分类方案应作为控制实施的依据，如访问控制、归档或加密。为了确定具体资产所需要的安全水平,就要对资产的敏感性和重要性进行粗略的评估。

在隐私方面,很多国家的法律、法规和其他规定都要求公共与私立机构保护个人数据的隐私性,以及信息系统和计算机系统的安全性。数据传输到云中后,保护数据安全的义务通常都由数据的收集人或管理人承担,尽管有些情况下收集人或管理人可能与其他人共同承担该义务。即使需要第三方托管或处理数据，数据管理人也应对数据的丢失、损坏或滥用负责。因此,数据管理人和云供应商签订书面(法律)协议是比较稳妥甚至是法律规定的做法,这样可以明确协议双方的职责和要求,并分割双方的相关责任。

6.明确服务管理要求

用户在与云供应商签订服务水平协议时需要考虑的有关服务管理的重要问题，主要包括审计、监控和汇报、计量、快速调配、资源变更、对现有服务的升级等方面。

7.为服务故障管理做准备

云SLA应明确书面记录预期的服务能力和服务性能,否则用户和供应商发生误会的可能性会显著增加。例如,除非SLA中有明确规定,否则供应商不会认为Webservice的响应时间过长属于服务故障。

服务故障管理的水平因供应商的不同而有很大差异,而能否争取到更高水平的管理服务则取决于用户公司的规模。因此用户应在协议中包括其自身的服务故障管理能力,以确保能够及时获知出现的问题。

8.了解灾难恢复计划

灾难恢复属于业务连续性的范畴，主要指在发生灾难时，用于恢复应用程序、数据、硬盘通信(如网络)和其他IT基础设施的流程与技术。这里的灾难既包括自然灾害，又包括影响IT基础设施或软件系统可用性的人为事件。

企业将IaaS、PaaS或SaaS外包到云环境并不意味着企业就不需要制订严格的灾难计划。每个企业外包的基础设施或软件的重要性不同，因此云灾难恢复计划也各不相同，而在制订灾难恢复计划时，业务目标是非常重要的参考。

9.建立有效的管理流程

不断发展的云计算需要有一套有效的管理流程,以解决可能遇到的各种问题。实行有效的管理流程是确保内部和外部用户对云服务的满意度的重要步骤。

一个成功的管理流程的重要环节主要包括确定每月例会,确保恰当的出勤、议题,追踪关键指标和生成报告。

10.了解退出流程

每个云SLA中都应包含退出条款,对退出流程进行详细规定,包括云供应商与用户的关系提前终止或到期终止时的责任分配。

SLA都要明确规定退出流程,确保安全快速地转移用户的数据和应用程序。用户退,出计划始终应在一开始签订SLA时就进行准备,并附在合同中。该计划应保证用户业务损失最小，并能顺利过渡。该退出流程应包括详细的程字,确保业务持续性,并明确提出可度量的指标,确保云供应商有效实施这些流程。

3.3.3 云安全实施步骤

- 当用户把其应用及数据转移到云计算时，在云环境中提供一个与传统IT环境一样或更好的安全水平至关重要。如果不能提供合适的安全保护，最终将造成更高的运营成本并有可能导致潜在的业务损失，从而影响云计算的收益。

1.确保拥有有效的风险治理策略及合规性流程

大多数机构已经为保护其知识产权和公司资产(尤其是在IT领域的资产)制定了安全及合规的策略与规程。对云计算环境的安全控制与传统IT环境下的安全控制是相似的,然而由于职责部门采用云服务和运维模型以及云服务所使用的技术等因素,云计算与传统IT解决方案相比会为机构带来不同风险。

依据安全和合规性政策,云服务用户保证其托管应用和数据安全的主要方式是参考相关的服务水平协议，核实用户和供应商之间的合同是否包含他们的所有要求。用户了解与安全性相关的所有条款,并确保这些条款能够满足其需要是至关重要的。如果没有合适的合同和SLA,那么不建议继续使用该机构的云服务。

2.审计运维和业务流程报告

- 用户至少应保证看到独立审计师编写的关于云服务供应商的运维报告。能够自由获取重要的审计信息是用户与任何云服务供应商签订合同和SLA条款时的关键因素。作为条款的一部分,云服务供应商应及时提供与用户相关的特定数据或应用程序审计事项，以及日志记录和报告信息,保证访问能力和自我管理能力。

2.审计运维和业务流程报告

主要从以下三个领域对云安全进行考虑。

(1) 了解云服务供应商的内部控制环境，包括其调配云服务时环境的风险控制及其他治理问题。

(2) 对企业审计跟踪的访问，包括当审计跟踪涉及云服务时的工作流程和授权。

(3) 云服务供应商应向用户保证云服务管理和控制的设施是可用的，以及说明该设施是如何保障安全的。

3.明确管理人员角色及身份

云用户必须确保其云服务供应商具备相关流程和功能来管理具有访问其数据与应用程序权限的人员，保证对其云环境的访问可控、可管理。云服务供应商必须允许用户根据其安全策略为每一个用户分配、管理角色和进行相关等级的授权。这些角色和授权以单个资源、服务和应用程序为基础。云服务供应商应包含一个安全系统来管理其用户和服务的唯一身份标识。这项身份管理功能必须支持简单的资源访问及可靠的用户应用程序和服务工作流。无论是何种角色或权限，供应商管理平台所有的用户访问或互操作行为都应该被监控并予以记录，以便为用户提供其数据和应用程序的所有访问情况的审计报告。

云服务供应商应设计正式流程，管理其员工对任何存储、传输或执行用户数据和应用程序的软硬件的访问情况，并应将管理结果提供给用户。

4.确保对数据和信息的合理保护

云计算中的数据问题涉及不同形式的风险，包括数据遭窃取或未经授权的披露，数据遭篡改或未经授权的修改，数据损失或不可用。“数据资产”可能包括应用程序或机器镜像等，与数据库中的数据和数据文件一样，这些资产也有可能遇到相同的风险。

我国国家标准《信息安全技术云计算服 务安全指南》和《信息安全技术云计算服务安全能力要求》对保障数据安全性、使用云服务时需要解决的数据安全注意事项等，从不同方面做了详细规定。

4.确保对数据和信息的合理保护

用户为确保云计算活动中的数据得到适当保护应注意以下几个方面。

(1) 创建数据资产目录。

(2) 将所有数据包含其中。

(3) 注重隐私。

(4) 保密性、完整性和可用性。

(5) 身份和访问管理。

5.实行隐私策略

在云计算服务合约和云SLA中有必要充分解决隐私权保护问题。如果不明确列明隐私问题，用户应考虑通过其他方式实现其目标，包括寻找其他供应商或不将敏感数据导入云计算环境。

用户有责任制定策略以处理隐私权保护问题，并在其机构内部提高数据保护意识，同时还应确保其云服务供应商遵守上述隐私权保护策略。用户有义务持续核对其供应商是否遵守了上述策略，包括涵盖隐私权保护策略等所有方面的审计项目（涉及确保供应商是否采取改进措施的方法）。

6.评估云应用程序的安全规定

- 制定明确的安全策略和流程，对确保应用程序能够帮助业务正常进行而避免额外风险至关重要。应用程序的安全性对云服务供应商和用户至关重要，与保障物理和基础设施安全性相同，双方机构应尽力保障应用程序的安全性。不同云部署模型下的应用程序安全策略均不相同，主要区别如下

1)IaaS

(1) 用户有责任部署完整的软件栈(包括操作系统、中间件及应用程序等)及与堆栈相关的所有安全因素。

(2) 应用程序安全策略应精确模拟用户内部采用的应用程序安全策略。

(3) 在通常情况下,用户有责任给操作系统、中间件及应用程序打补丁。

(4) 应采用恰当的数据加密标准。

2)PaaS

(1) 用户有责任进行应用程序部署，并有责任保证应用程序访问的安全性。

(2) 供应商有责任合理地保障基础设施、操作系统及中间件的安全性。

(3) 应采用恰当的数据加密标准。

(4) 在PaaS模式下，用户可能了解也可能不了解其数据的格式和位置，但用户应被告知获得管理访问权限的个人将如何访问其数据。

3)SaaS

(1)应用程序领域安全策略的限制通常是供应商的责任并取决于合约及SLA中的条款。用户必须确保这些条款满足其在保密性、完整性及可用性方面的要求。

(2)了解供应端的修补时间表,恶意软件的控制及发布周期十分重要。

(3)阈值策略有助于确定应用程序用户负载的意外增加和减少,阈值以资源、用户和数据请求为基础。

(4)在通常情况下,用户只能够修改供应商已公开的应用程序参数,这些参数可能与应用程序的安全配置无关,但用户应确保其配置更改不会妨碍供应商的安全模式。

(5)用户应了解其数据如何受到供应商管理访问权限的保护。在SaaS模式下,用户可能并不了解其数据存储的位置和格式。

(6)用户必须了解适用于其静态和动态数据的加密标准。

7.确保云网络和连接的安全性

- 云网络和连接的安全性分为外部网络安全与内部网络安全两部分。建议从流量屏蔽、人侵检测防御、日志和通知等方面来评估云服务供应商的外部网络管理。内部网络安全与外部网络安全不同，在用户得以访问云服务供应商的部分网络后，维护内部网络安全由云服务供应商负责。用户应关注的主要内部网络攻击包括保密性漏洞（敏感数据泄露）、完整性漏洞（未经授权的数据修改），以及可用性漏洞（有意或无意地阻断服务）。用户必须根据其需求和任何现存的安全策略评估云服务供应商的内部网络管理。建议从保护用户不受其他用户攻击、保护供应端网络和检测入侵企业等方面，对云服务供应商的内部网络管理进行评估和选择。

8.评估物理基础设施和设备的安全管理

云服务供应商应采用的适用于物理基础设施和设备的安全管理包括如下内容。

(1)物理基础设施和设备应托管在安全区域内。应设置物理安全界限以防止未授权访问,并配合物理准人控制设施以确保只有获得授权的人员才能访问包含敏感基础设施的区域。所有与安装和调配云服务相关的物理基础设施的办公室房间或设备都应设置物理安保措施。

(2)应针对外部环境威胁提供安全措施,火灾、洪灾、地震及其他潜在威胁都有可能破坏云服务,因此应对上述威胁提供安保措施。

(3)应对在安全区域工作的员工进行管理。这类管理的目的在于防止恶意行为。

(4)应进行设备安全管理,以防止资产丢失、被盗、损失或破坏。

(5)应对配套公共设施进行管理,包括水、电、气的供应等。应防止由服务失败或设备故障(如漏水)导致的服务中断。应通过多路线和多个设备供应商保证公共设施正常运作。

8.评估物理基础设施和设备的安全管理

(6)保障线缆安全，尤其要保障动力电缆和通信线缆的安全，以防止意外或恶意

(7)应进行适当的设备维护，以确保服务不会因可预见的设备故障而中断。

(8)管理资产搬迁，以防止重要或敏感资产遭盗窃。

(9)保障废弃设备或重用设备的安全，这一点对可能包含存储媒体等数据的设备尤为重要。

(10)保障人力资源安全，应对在云服务供应商的设施内的工作人员进行管理，包括任何临时或合约员工。

(11)备份冗余和持续服务计划。供应商应提供适当的数据备份、设备冗余和持续服务计划以应对可能发生的设备故障。

9.管理云SLA的安全条款

- 云活动中的安全责任,必须由云服务供应商和用户双方,通过云SLA的条款来共同明确和承担,SLA保障安全的一大特征是,SLA对云服务供应商提出要求,该供应商为提供服务而可能会使用到的其他云服务供应商也必须遵守SLA。

10.了解退出过程的安全需要

- 用户退出或终止使用云服务的过程需要认真考虑安全事项。从安全性角度出发，当用户完成退出过程后，用户具有“可撤销权”，云服务供应商不可继续保留用户的数据。供应商必须保证数据副本已经从服务商环境下可能存储的位置（包括备份位置及在线数据库）彻底清除。同时，除法律层面需保留的用户数据可暂时保留一段时间外，其他与用户相关的数据信息（日志或审计跟踪等），供应商应全部清除。

思考与练习

1. 简要描述云计算实施的主要过程。
2. 简要描述云SLA实施的步骤。