

网络安全信息简报

安博士月刊

2014.06 (Vol.20)

云计算(Cloud Computing)



理解云计算

通过数字说云计算

2006年8月9日，Google首席执行官埃里克·施密特（Eric Schmidt）在搜索引擎大会（SES San Jose 2006）首次提出“云计算”（Cloud Computing）的概念。Google“云端计算”源于Google工程师克里斯托弗·比希利亚所做的“Google 101”项目。云计算概念的出现，给IT行业带来了最热门的话题。¹

有些人把云计算表现为Life革命而不是IT革命。此概念出现以后，成为了国际调查机关每年发表的年终IT趋势报告里的热门主题。直到2014年现在，仍然是受到注目的主题。IT行业人士都听说过云计算并略知一点，但是要真正理解并非易事。

本刊为了有助于理解云计算的概念，将详细介绍云计算的概念和特点。

宾馆和住宅，您会选择哪个？

如果有宾馆和住宅让您选择居住，您会选择哪个？这有可能是一个愚蠢的问题。根据所处的情况不同，选择也可能有所不同。对于短期居住的人，可能会选择宾馆；如果长期居住的话，可能会选择住宅。那么住宅和宾馆各有什么样的好处和坏处？首先，住宅是个人空间，不会有人来打扰，还可以保障隐私。但是，需要定期支付电费、水费等各种管理费用，不仅自己打扫卫生和维修房屋，还要防备小偷和强盗的入侵。

与住宅相比，宾馆就不用自己打扫卫生并且不用管理房屋的维修，每天由服务员更换床单和打扫房间，也不用费心电费、水费等管理费用。尽管宾馆有很多好处，但是宾馆里的所有东西最终都不是个人所有，而且服务员要来房间打扫卫生，这可能让你担心个人隐私。

如此，宾馆和住宅各有各的好处，最终选择还是由各自的情趣。但，假设下面的特别情况后再来选择一下，可能结果会不同。假设您的家里经常有数十名的客人突然来访问，并逗留几天。此时，宾馆和住宅您会选择哪个？(为避开极端的事例，设定住宅面积为130m，共有4个房间和1个客厅。)这时候，大部分的人可能会选择宾馆。

IT系统也有如宾馆的服务。只要支付一定的费用，不管是服务器、存储设备或网络都可以增加后使用。还可以租用软件开发所需的框架，或不需要开发软件，而直接租用高品质的软件。

用户支付费用只享受服务，而不知道该服务系统内部是如何构成。虽然不清楚云后面的内部，但是正常运行的高品质的计算服务，被称为云计算（Cloud Computing）。

如果把云比喻成宾馆，那么企业自主运营的IT系统可以比喻成单独住宅。如同一起住在住宅的家族各自使用一个房间，构成企业IT系统的服务也各自独占特定的服务器使用。

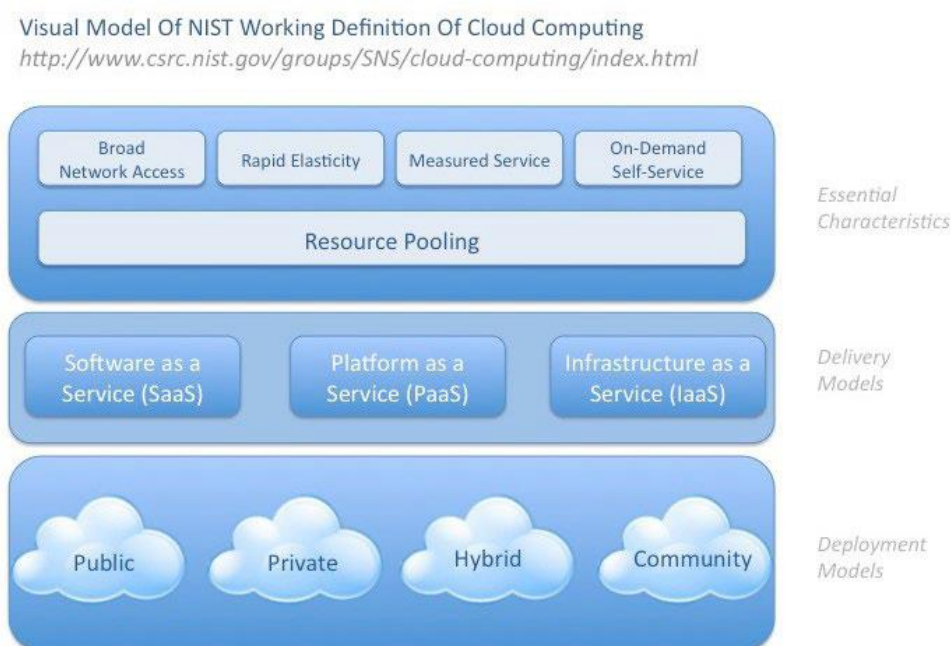
¹ 百度百科，http://baike.baidu.com/link?url=PsnsEHDtGGssPFgDCpyy0u1aaNuTdtv65btmBvUZ0ExH3fzq-lo9w8tWhpyA1N_x8dnmJSbz_QFSROGDbbhYCa

这种单独住宅型IT系统平时也无碍正常运行。但是，如果突然有大量流量来访问会怎样？例如，购物网站在节日期间会发生平时几倍的流量，安全提供商如果发生安全事故，流量也会暴增。您会想：如果来访的客人多，那么增加房间不就可以？但是，在极短的时间内增加房间是很困难的一件事情。企业IT系统也一样，即使流量暴增，在很短的时间内增加服务器并非易事。更何况，流量暴增的问题应付几天便可以解决。为了应付几天而增设平时几倍的服务器，这划算吗？这样的情况下，像宾馆的云服务可以说是卓越的解决方案。短时间来访的客人多的时候，根据需要租用房间并支付相应的费用即可。

目前的IT环境与以前企业服务为目的运营相比变得非常复杂。服务种类也变得多样，很难预测网络流量的变化。从方便性角度来看，自己拥有并管理的系统方便；从迅速且弹性响应复杂环境和急剧变化的角度来看，云系统绝对优势。因此，包括世界IT调查机关Gartner的年终IT趋势预测报告的各种IT趋势报告中，云计算已成为了不可缺少的一个主题。下面，让我们来仔细了解一下有关云计算的主要概念。

了解云计算的数字 5, 4, 3

作为云的标准流传最广的资料是美国国家标准与技术研究所(NIST,U.S. National Institute of Standards and Technology)的 NIST Working Definition of Cloud Computing(NIST 800-145)。NIST将云计算定义为5个基本特征、4个部署模型和3个服务模型。



云计算定义的直观模型（来自：CSA云计算关键领域安全指南v3.0）

5：云计算的五个特征²

1) 资源共享池(Resource Pooling)

服务提供者将计算资源汇集到资源池中，通过多租户模式共享给多个消费者，根据消费者的需求对不同的物理资源和虚拟资源进行动态分配或重分配。资源的所在地具有保密性，消费者通常不知道资源的确切位置，也无力控制资源的分配，但是可以指定较精确的概要位置（如，国家、省、或数据中心）。资源类型包括存储、处理、内存、带宽、和虚拟机等。

2) 无处不在的网络访问(Broad Network Access)

² CSA云计算关键领域安全指南v3.0

网络中提供许多可用功能，可通过各种统一的标准机制从多样化的瘦客户端或者胖客户端平台获取（例如，移动电话、笔记本电脑、或PDA掌上电脑）。

3) 按需应变的自助服务(On-demand Self service)

消费者可以单方面地按需自动获取计算能力，如服务器时间和网络存储，从而免去了与每个服务提供者进行交互的过程。

4) 快速而灵活(Rapid Elasticity)

能够快速而灵活地提供各种功能以实现扩展，并且可以快速释放资源来实现收缩。对消费者来说，可取用的功能是应有所尽有的，并且可以在任何时间进行任意数量的购买。

5) 计量付费服务(Measured Service)

云系统利用一种计量功能（通常是通过一个付费使用的业务模式）来自动调控和优化资源利用，根据不同的服务类型按照合适的度量指标进行计量（如，存储、处理、带宽和活跃用户账户）。监控，控制和报告资源使用情况，提升服务提供者和服务消费者的透明度。

4：云计算的四个部署模型

1) 公共云(Public Cloud)

2) 私有云(Private Cloud)

3) 社区云(Community Cloud)

4) 混合云(Hybrid Cloud)

云计算服务的优点是将资源灵活分配给多数用户。但，另一方面该优点也成为了不愿意使用云计算服务的最大原因。如果管理云服务的消费者和共享云服务的消费者都不是同一公司的人，该服务如何叫人放心使用？而且如何保证共享云服务的消费者中没有黑客或者网络犯罪集团？为解决用户所忧虑的这点而出现的模型，便是“私有云(Private cloud)”。它保留了云计算服务的所有优点，并解决了其他组织访问的安全问题。与此相反，收费提供的共享资源运营的方式，便是“公共云(Public cloud)”。云计算系统一旦构筑，响应各种要求的灵活性很强。但是不管怎样，在初期的构筑过程中需要大改革水准的工作。而且，如要发挥云计算的优点，需要确保一定水准的系统闲置空间，这些部分单独一个人或公司负担也不是件小事。因此，一些由有着共同利益并打算共享基础设施的组织共同创立云，该方式即被称为“社区云(community cloud)”。最后，根据企业的需要混用公共云、私有云和社区云，该方式称为“混合云(Hybrid cloud)”。

3：云计算的三个服务模型³

1) 软件即服务 (SaaS)

该模式的云服务，是在云基础设施上运行的、由提供者提供的应用程序。这些应用程序可以被各种不同的客户端设备，通过像Web浏览器（例如，基于Web的电子邮件）这样的瘦客户端界面，所访问。消费者不直接管理或控制底层云基础设施，包括网络，服务器，操作系统，存储，甚至单个应用的功能，但有限的特定于用户的应用程序配置设置则可能是个例外。

2) 平台即服务(PaaS)

该模式的云服务，是将消费者创建或获取的应用程序，利用资源提供者指定的编程语言和工具部署到云的基础设施上。消费者不直接管理或控制包括网络，服务器，运行系统，存储，甚至单个应用的功能在内的底层云基础设施，但可以控制部署的应用程序，也有可能配置应用的托管环境。

3) 基础设施即服务 (IaaS)

该模式的云服务，是租用处理、存储、网络和其他基本的计算资源，消费者能够上面部署和运行任意软件，包括操作系统和应用程序。消费者不管理或控制底层的云计算基础设施，但可以控制操作系统、存储、部署的应用，也有可能选择网络构件（例如，主机防火墙）。

³ CSA云计算关键领域安全指南v3.0

引进云计算时需要考虑的14个安全因素

目前最鲜为人知的云计算安全组织非CSA(Cloud Security Alliance)莫属。CSA是非盈利团体不是属于特定国家的机关，全世界约有5万名会员，成立目的是为了在云计算环境下提供最佳的安全方案。CSA发布的最新的安全指南版本是v3.0，该指南分为14个域提示了云安全关键因素。当使用公共云或者构筑私有云的时候，参考该安全指南会有很大的帮助。(参考：<https://cloudsecurityalliance.org/research/ccm/>)

域	指南涉及...
01 云计算体系架构	该部分已在前面说明的“了解云计算的数字 5, 4, 3” 部分的内容相同。 根据云服务的展开模型和提供的模型，用户所负担的安全领域不同，并且应用安全的过程也有所差异，解说云计算的基本结构和差异。
02 治理与企业风险管理	组织治理和度量云计算带来的企业风险的能力。 例如违约的判决先例，用户组织充分评估云提供商风险的能力，当用户和提供商都有可能出现故障时保护敏感数据的责任，及国际边界对这些问题有何影响等都是关注点。
03 法律问题： 合同与电子发现	使用云计算时潜在的法律问题。 本节涉及的的问题包括信息和计算机系统的保护要求、安全漏洞信息披露的法律、监管要求，隐私要求和国际法等。
04 合规与审核	保持和证明使用云计算的合规性。 本节涉及评估云计算如何影响内部安全策略的合规性、以及不同的合规性要求（规章、法规等）。同时还提供在审计过程中证明合规性的一些指导。
05 信息管理与数据安全	管理云中的数据。 本节涉及云中数据的识别和控制；以及可用于处理数据迁移到云中时失去物理控制这一问题的补偿控制。也提及其它项，如谁负责数据机密性、完整性和可用性等。
06 互操作性与可移植性	将数据或服务从一个提供商迁移到另一个提供商，或将它全部迁移回内部的能力。提供商间互操作性相关的问题也在这节讨论。
07 传统安全，业务连续性和灾难恢复	云计算如何影响当前用于实现安全性、业务连续性和灾难恢复的操作流程和规程。关注点是讨论和检查云计算的潜在风险，希望增加针对企业风险管理模式巨大需求的对话和讨论。进而，本节还讨论了如何帮助人们识别云计算在那些方面可以有助于减少安全风险，而在某些领域则增加了风险。
08 数据中心运行	如何评估提供商的数据中心架构和运行。主要关注帮助用户识别对持续服务不利的常见的数据中心特征，以及有助于长期稳定性的基础特征。
09 事故响应	适当的和充分的事件检测、响应、通告和补救。尝试说明为了启动适当的事件处理和取证，在用户和提供商两边都需要满足的一些条目。本域将会帮助您理解云给您现有的事件处理程序带来的复杂性。

10 应用程序安全	保护在云上运行或在云中开发的应用软件。包括将某个应用迁移到或设计在云中运行是否可行，如果可行，什么类型的云平台是最合适的（ SaaS, PaaS, or IaaS ）。
11 加密与密钥管理	识别恰当的加密使用方法以及可扩展的密钥管理。本节并不是什么规范，而是提供更多信息来探讨为什么需要这些方法，识别使用过程中出现的问题，包括保护对资源的访问以及保护数据。
12 身份、授权和访问管理	管理身份和利用目录服务来提供访问控制。关注点是组织将身份管理扩展到云中遇到的问题。本节提供洞察评估一个组织准备就绪进行基于云的身份、授权和访问管理(Id EA)。
13 虚拟化	虚拟化技术在云计算中的应用。本节论述了与多租户、VM 隔离、VM共居（ co-residence ）、Hypervisor脆弱性相关联的风险。本域更关注系统和硬件虚拟化相关的安全问题，而不是对各种形式虚拟化的泛泛纵览。
14 安全即服务 (Security as a Service)	提供第三方促进安全保障、事件管理、合规认证以及身份和访问监督。安全即服务是将安全基础设施的检测、修复和治理委托给一个具备恰当的工具和专业知识的可信第三方。这种服务的用户可以得益于在保护和加固敏感业务运作中获得专门的专业知识和前沿技术。

到目前为止，大概了解了云计算的概念和特征，还有关键因素。圣经中有句话‘太阳之下无新的东西’，云计算的概念也如此，不是突然间蹦出来的完全陌生的概念，而是过去优秀的多种技术积蓄而构成了云技术的特征，最终诞生了云计算概念。我们期待读者对云技术持有关心并积极利用该技术的优点。AhnLab 也作为综合网络安全公司，向用户承诺：积极利用云技术，为提供更方便有效的安全服务而倍加努力。



<http://www.ahn.com.cn>
<http://global.ahnlab.com>
<http://www.ahnlab.com>



关于安博士 (AhnLab, Inc.)

安博士的尖端技术和服务不断满足当今世界日新月异的安全需求，确保我们客户的业务连续性，并致力于为客户提供一个安全的计算环境。我们提供全方位的安全阵容，包括经过证实的适用于桌面和服务器的世界级防病毒产品、移动安全产品、网上交易安全产品、网络安全设备以及咨询服务。

安博士已经牢固地确立了其市场地位，其销售伙伴遍布全球许多国家和地区。

AhnLab

北京市朝阳区望京阜通东大街1号院望京SOHO220502室 | 上海市闵行区万源路2158号18幢泓毅大厦1201室

电话：+86 10 8260 0932 / +86 21 6095 6780 | v3site@ahn.com.cn

© 2014 AhnLab, Inc. All rights reserved.