云计算下的安全架构 v1

薛润忠

2012 年 3 月

目　　录

第一章 概述

目前，云计算产业受到业界的极大推崇并推出了一系列基于云计算平台的服务。但在已经实现的云计算服务中，安全问题一直令人担忧。

例如，微软云计算平台 WindowsAzure 运作的中断，亚马逊的"简单存储服务"（Simple StorageService,S3）两次中断，导致依赖于网络单一存储服务的网站被迫瘫痪，S3 问题阻止了新虚拟机在计算云上的注册，以至于有些虚拟机无法启动，凡此种种，都属于可用性和可靠性问题。当然这类问题的背后，有可能是微软、亚马逊的安全措施没有到位，遭受了黑客的攻击所致；也可能是系统自身的可靠性没有得到充分保证所致。但其表现出来的问题不是我们传统意义上的安全问题，而是可靠性和可用性问题。这里我们姑且将之纳入到广义的云安全里。

谷歌邮箱再次爆发大规模的用户数据泄漏事件，大约有 15 万 Gmail 用户在周日早上发现自己的所有邮件和聊天记录被删除，部分用户发现自己的帐户被重置，谷歌表示受到该问题影响的用户约为用户总数的 0.08%。

2011 年 1 月 21 日，来自研究公司 ITGI 的消息称，考虑到自身数据的安全性，很多公司正在控制云计算方面的投资。在参与调查的 21 家公司的 834 名首席执行官中，有半数的官员称，出于安全方面的考虑，他们正在延缓云的部署，并且有三分之一的用户正在等待，安全和隐私问题已经成为阻碍云计算普及和推广的主要因素之一，所以推出有效的云安全方案已经是迫在眉捷的问题

本文将从技术和非技术两个方面试图阐述如何保障云计算环境下的安全，包括网络层和网络层以上的应用的安全，就技术层面而言，云安全的保障在于两个方面，一个是在分布式环境下的数据安全保障，第二个方面是解决虚拟机的安全问题。

第二章 需求分析，方案范围及目标

云计算应用有公有云和私有云之分，考虑未来几年主要是发展私有云的建设和发展，因此本文主要考虑私有云的安全架构。

云计算的主要风险点可归纳如下：

1.资源和数据外包

企业的资源和数据置于共享公共网络上，置于企业边界之外。云计算这种全新的服务模式将资源的所有权、管理权及使用权进行了分离，因此用户失去了对物理资源的直接控制，会面临与云服务商协作的一些安全问题。同时，越来越多的数据存于“云”中，就意味着有越多的数据被滥用的可能。如果只是不重要的数据，企业对于其关注度也没那么大；如果是机密数据，也就是属于企业隐私，这些资料被盗，对于企业的打击则非常大，这也是很多企业至今不敢尝试云计算的原因。

2.云计算服务商的可靠性

理想情况下，你的云计算服务商绝不会破产或被一家较大的公司收购和吞并。你必须确定数据在发生了此类事件后仍能继续使用。要询问可能的云计算服务商，怎么才能要回你的数据，数据格式是否可以让你能够导入到替代的应用之中。

3.多租户环境

数据在云中通常是处在一个和其他客户的数据共享的环境中。加密虽然是有效的，但并不是万能灵丹，因此要找出你的数据在休眠时是否做了隔离。云计算平台上集成了多个租户，多租户之间的信息资源如何进行安全隔离、服务专业化引发的多层转包导致的安全问题等。

4.动态的信任边界

企业的信任边界是动态的，企业无法确定信任边界的变动情况。客户在使用云计算时，可能无法确切地知道你的数据到底被托管在什么地方。事实上，你甚至可能不知道这些数据存放在了哪个国家，也可能遍布在不断变化的一组主机和数据中心中。

5.缺乏透明性

云计算服务商的安全控制和实施缺乏透明性，大多数云服务商在服务水平协议、提供商管理功能以及安全责任这些领域缺乏透明度。如云计算服务软件的漏洞对云计算用户并不是透明的，这就阻碍了用户对与漏洞相关的运行风险的管理。

6.云计算管理标准缺乏

云计算服务商必须遵守各种不同的 IT 流程控制和管理需求，包括外部需求和内部需求，可以通过联合的合规工作以处理所有这些需求，使用更加统一和有策略的方法，从而提高效率并满足合规性，同时实现不同云计算间的无缝互通。而目前各类云计算标准还很缺乏，使得企业改变云服务商变得非常困难。

一个安全的信息系统不仅仅要考虑环境安全和技术安全，还要考虑管理安全；不仅仅能够提供静态的保护能力，包括防止和降低故障、损害，还需要具备主动防御的能力，能够及时发现攻击，并能够从破坏中恢复。对于云计算数据中心的安全保护，通过单一的手段是远远不够的，需要有一个完备的体系，涉及多个层面，需要从法律、技术、监管三个层面进行。

目前云计算的安全问题是绝对存在的，但随着云计算技术的发展，实现对云计算更好的了解、更多的透明度以及更好的安全技术能力，云计算安全方面的顾虑与声音将会逐步消失。

云计算安全和传统 IT 安全两者有很多相同之处，它们最终的目标都是为了保护数据的完整性，保护的对象也都是计算资源、存储资源和网络资源。但由于云计算的不同特性，除传统的 IT 防护技术外，应该针对云计算数据中心安全的特点加以考虑。

第三章 设计依据、原则

3.1 可用性（Availability）

3.1.1 给云终端提供及时有效的服务

可访问，及时性是云服务的基本要求，云计算平台的健壮性因此非常重要，我们在选择云平台的时候首先选择稳定性强的平台，因此各项测试是必须的。云中利用防火墙，IDS，IPS，防攻击，利用分布式安全软件防，杀病毒和垃圾数据，在基础网络层到云服务的最外层，采取多种安全措施保证数据的可用性：ACL，DHCP SPOOF I NG，NETFLOW，D A R P - Inspection 等等

下图是一个可能的云平台组织结构：

3.1.2 易管理维护

易管理维护意味着在云数据中心提供统一的分配使用资源的管理界面，包扩统一的账号系统，日志系统，网络管理分配界面，计算资源统一调配界面，存储统一调度界面，安全管理系统等。

3.2 可靠性（Reliability）

提供 数据的完整性，可靠性。要求系统不可抵赖，建立一套安全认证系统和日志管理系统

3.3 安全性（Security）

数据的私密性：关键数据加密存储

数据的安全访问：采用安全的方式连接

可扩展升级，异地备份，非改写权限保证

内部 Security：云计算厂商采用分权分级管理。为了防止云计算服务平台供应商"偷窥"客户的数据和程序，可以采取分级控制和流程化管理的方法。银行是一个很好的例子，银行虽然储存着所有客户银行卡的密码，但即使是银行内部员工，也无法获取客户的密码信息；同时，银行系统内也有一系列流程防止出现"内鬼".例如，将云计算的运维体系分为两级，一级是普通的运维人员，他们负责日常的运维工作，但是无法登录物理主机，也无法进入受控的机房，接触不到用户数据；二级是具备核心权限的人员，他们虽然可以进入机房也可以登录物理主机，但受到运维流程的严格控制。

第四章 云安全非技术考虑

4.1 法律法规层面的保障

国家制定必要得法律程序来约束云服务和用户的行为是云安全下的基本保障。

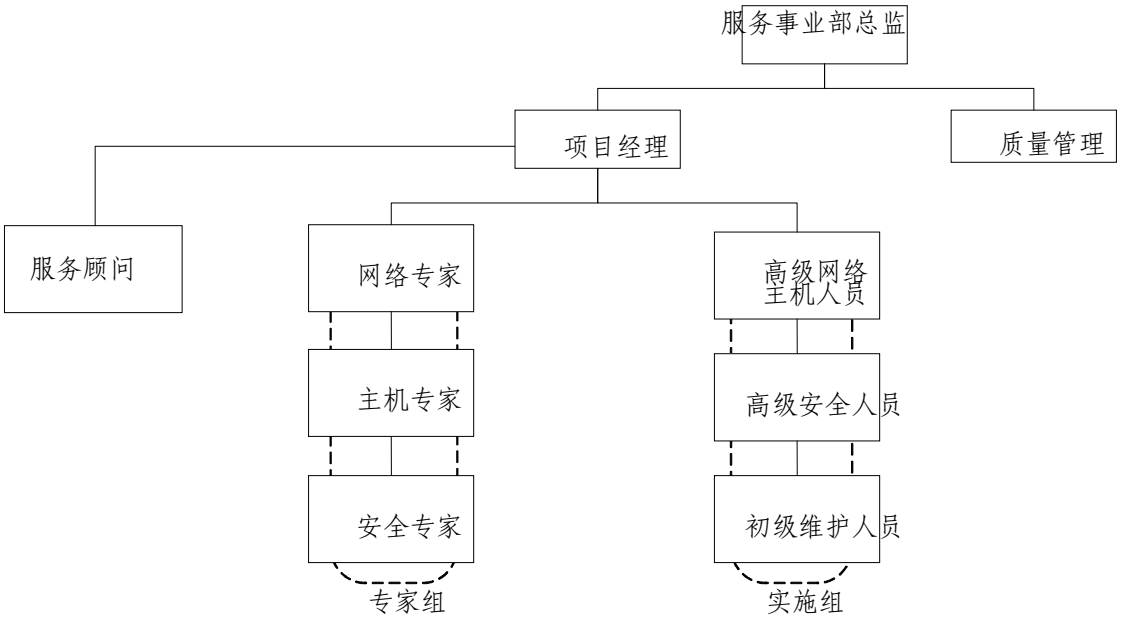
技术不是万能的，尤其是对于安全领域而言更是如此。因此，一些传统的非技术手段仍然可以被采用，以约束云服务商，从而确保云的安全性。常采用的非技术手段有第三方认证和合同约束。

第三方认证是提高信任关系的一种非常有效的手段。第三方认证是采用一个中立机构来对双方进行约束，中立机构必须具备很好的公信力，而且不会 被任何一方所左右，在安全领域有着丰富的经验和技术能力。中立机构的作用是对云服务商进行安全认证，采用标准化的技术和非技术手段对云服务商进行检测，试 图找出安全漏洞并对云服务商做出评价。微软已经在 2009 年请 VeriSign 公司为其 Windows Azure 平台提供基于云计算的安全和认证服务。

对于商业运营而言，从合同角度对云计算的安全性做一个约束是必须的。目前很多云服务商也提出了自己的云计算服务水平协议，从服务质量、技术 支持等方面对服务进行了量化，对合同双方的权利和义务进行了明确。例如 Amazon S3 的服务水平协议承诺在一个日历月的 99.5%时间内 S3 都会响应服务请求，EC2 承诺在一个地区内至少有两个可用性区域保证 99.95%的可用性。

4.2 人员制度管理方面

人员管理是安全管理的核心，只有做好人员的管理，在非技术层面的安全管理才能得到保障，下图是一个可能的组织结构：



服务顾问：　　人

项目经理：　　人

资深专家：　　人

技术工程师：　人

驻场维护人员：人

质量管理：　　人

人员职责：

任务	内容	工作时间	人员
顾问	提供优化建议、方案审查	定期	顾问
项目协调处理	项目规划、管理控制	全部	项目经理
高级安全服务	处理应急故障，体系规划，运维分析，建立各种优化方案，提供总体安全分析报告	定期，应急响应	资深专家
运维服务	处理一般故障和维护，优化方案实施，分析安全设备性能，提供系统运行维护报告	故障处理	技术工程师
现场监控服务	现场监控	7×24 现场	现场维护人员
质量管理	依照服务标准以及用户反馈对流程，	每月一次汇报，5×	质量管理

	工作成果、实施情况进行评价	9 接受投诉	人员

4.3 其他方面

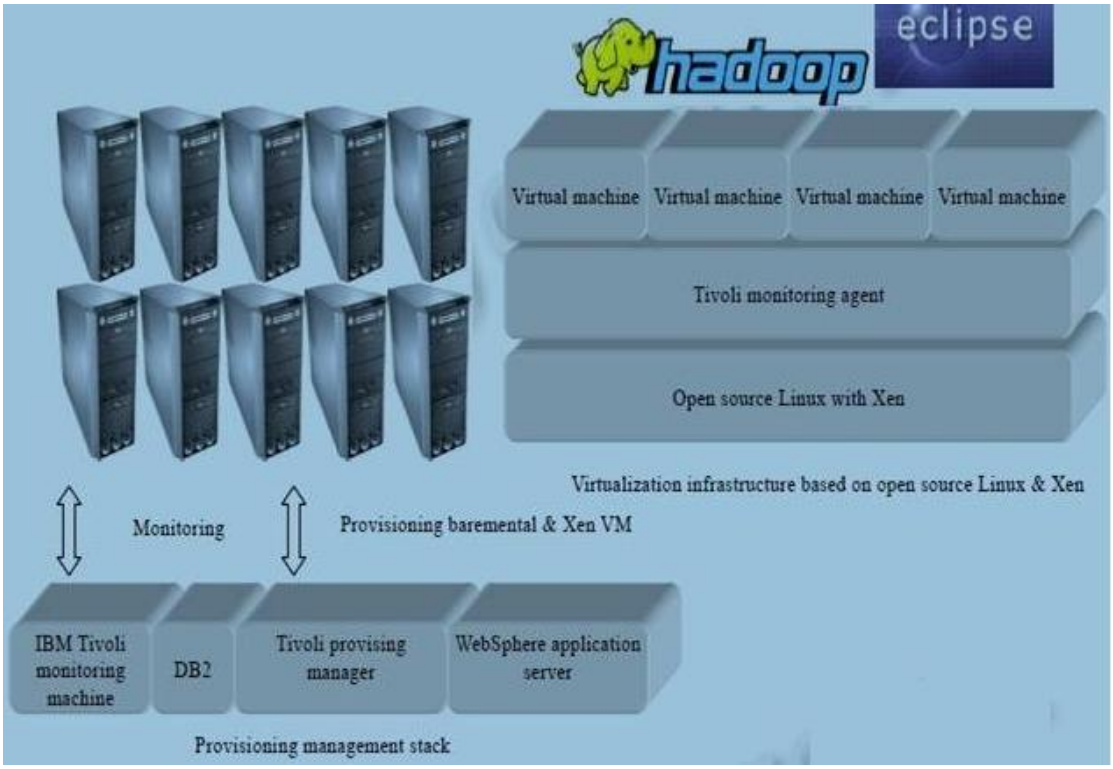
像机房制度管理等非技术层面的防范规范同样是要考虑的因素，本文不做重点，有兴趣的读者可以查阅相关文档资料。

第五章 云安全技术架构

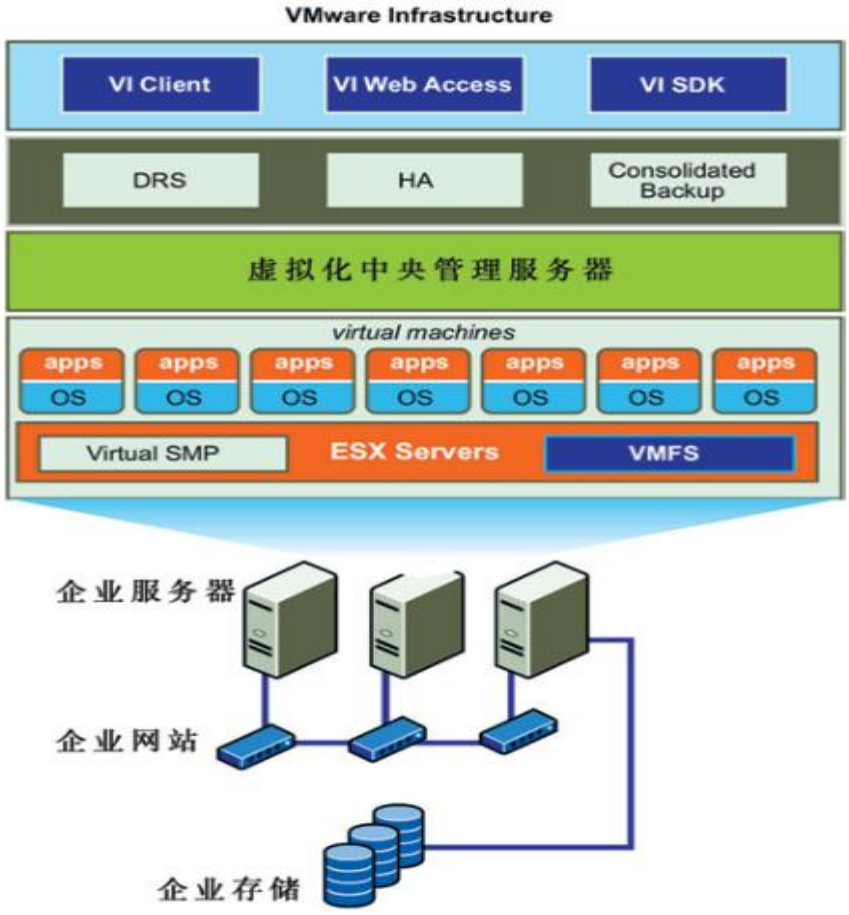
5.1 构建一个好的云计算平台

为了保证云服务的可用性，云平台的软、硬件架构需要足够健壮，例如 VMware 的 vSphere。IBM 的“蓝云”。

下图是 IBM 的云平台架构：

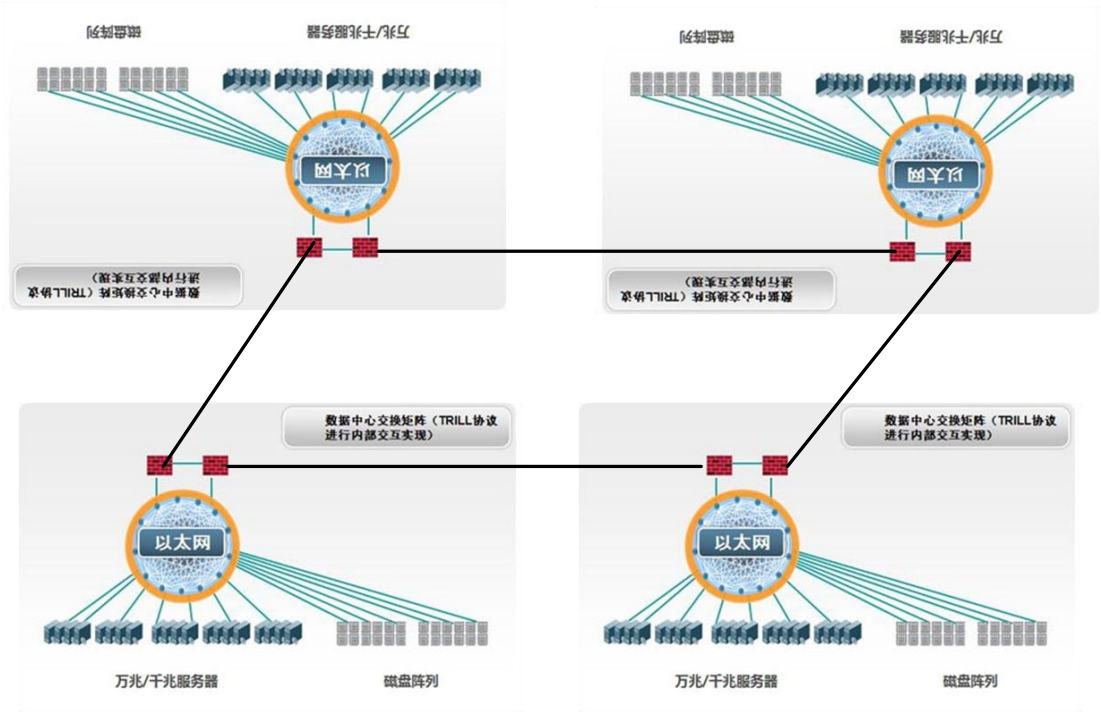


下图是 VMware 云平台架构：



5.1.2 云平台硬件架构

云平台的硬件拓扑：



未来数据中心会集成一系列的新技术，高带宽，低延迟，不丢包的路由和交换设备，大二层和扁平化技术是个趋势。分布式网络，分布式计算资源和分布式存储资源将会被统一调度和使用。

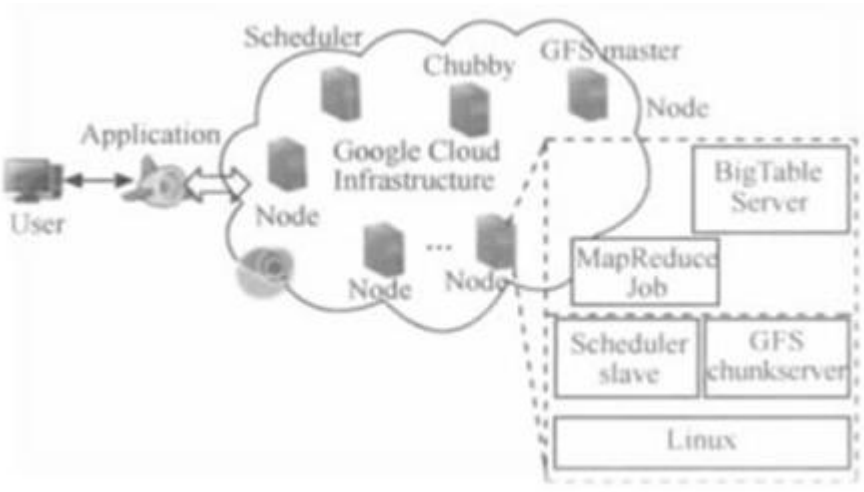
云计算网络安全集中 DC 的外部，通常是 Firewall，IPS，IDS 等的集成，GNFW 是发展的趋势，而在ＩＤＣ内部，如果采用硬件交换矩阵则不需做安全策略，如果是ＴＲＩＬＬ，则在运行ＴＲＩＬＬ的设备上运行安全控制策略（比如ＡＣＬ）

5.1.2 云平台软件架构

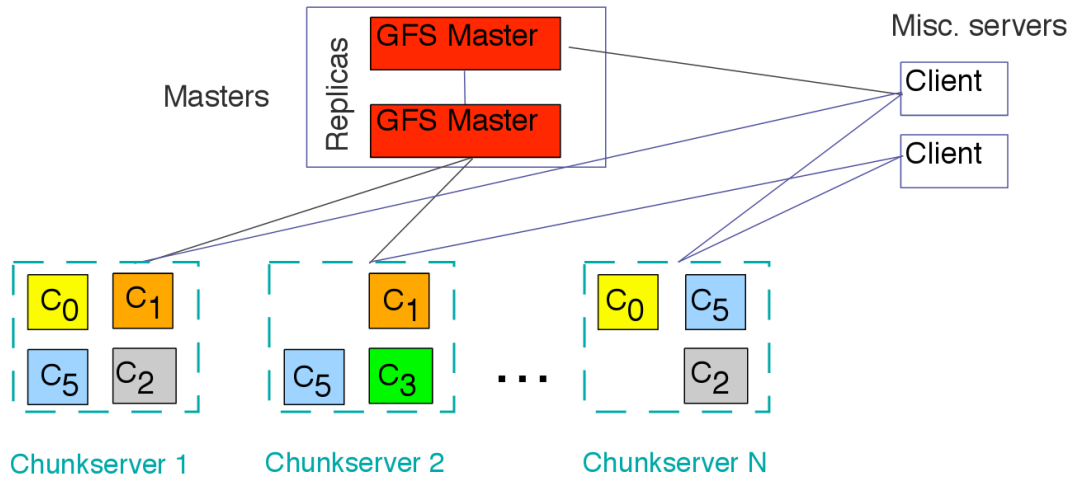
云平台操作系统是为了满足大量的，可并行的同构数据处理的要求，比如在互联网上的信息查询。而对于大型垂直数据处理或者不方面分拆的数据处理，像气象数据，科学计算，地震资料的数据处理更依赖于网格计算技术，网格计算与云计算的比较如下，网格计算不是本文讨论的内容。

谷歌的云计算系统是最早公布的，它包含几个部分，分布式计算系统 MapReduce，分布式文件系统 GFS 和分布式存储系统 Bigtable 以及一个同步系统 Google Chubby 分布式锁服务

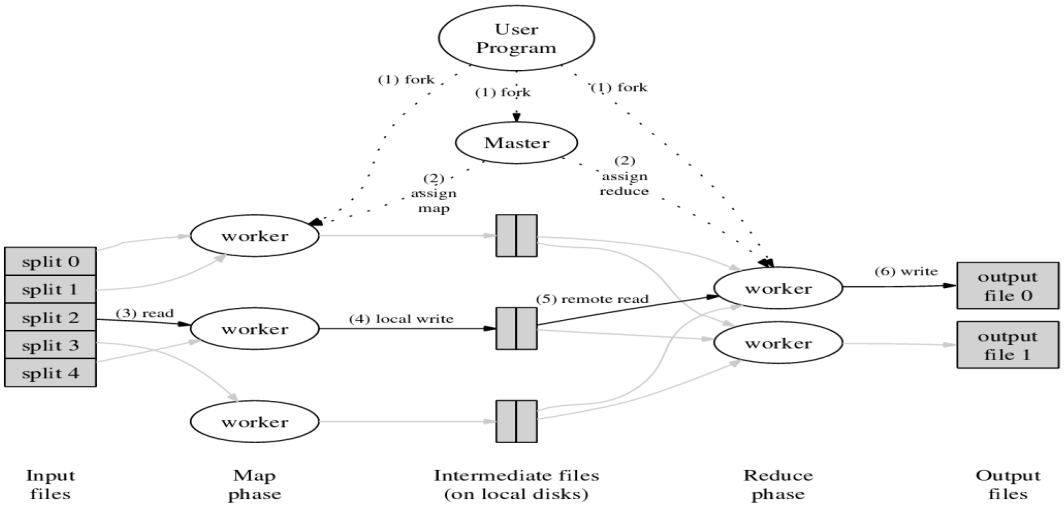
GOOGLE 云计算技术架构：



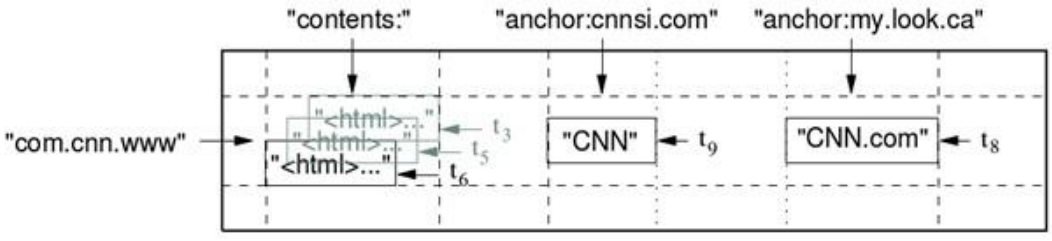
下图就是 GFS 的架构图：



下图为 MapReduce 的运行机制：



BigTable 数据模型图：



5.2 云数据中心互连安全

在各云数据中心外部署云火墙 C-NGFW（Cloud-Next Generation Firewall），用于保证云中心的安全，云火墙至少有以下四个特征：

A．拥有传统防火墙功能：C-NGFW 拥有传统防火墙所提供的所有功能，如基于连接状态的访问控制、NAT、VPN 等等。虽然我们总是在说传统防火墙已经不能满足需求，但它仍然是一种无可替代的基础性访问控制手段。

B．支持与防火墙自动联动的集成化 IPS：在同一硬件内集成 IPS 功能是必须的，但这不是 Gartner 想表达的重点。C-NGFW 内置的防火墙与 IPS 之间应该具有联动的功能，例如 IPS 检测到某个 IP 地址不断地发送恶意流量，可以直接告知防火墙并由其来做更简单有效的阻止。这个告知与防火墙策略生成的过程应当是由 C-NGFW 自动完成的，而不再需要管理员介入。比起前些年流行的传统防火墙/IDS 间的联动机制，这次升级并不是一个特别高深的技术进步，但我们必须承认它能让管理和安全业务处理变得更简单、高效。

C．应用识别、控制与可视化：C-NGFW 必须具有与传统的基于端口和 IP 协议不同的方式进行应用识别的能力，并执行访问控制策略。例如允许用户使用 QQ 的文本聊天、文件传输功能但不允许进行语音视频聊天，或者允许使用 WebMail 收发邮件但不允许附加文件等。应用识别带来的额外好处是可以合理优化带宽的使用情况，保证关键业务的畅通。虽然严格意义上来讲应用流量优化（俗称应用 QoS）不是一个属于

安全范畴的特性，但 P2P 下载、在线视频等网络滥用确实会导致业务中断等严重安全事件。

D．智能化联动：获取来自“防火墙外面”的信息，作出更合理的访问控制，例如从域控制器上获取用户身份信息，将权限与访问控制策略联系起来，或是来自 URL Filter 判定的恶意地址的流量直接由防火墙去阻挡，而不再浪费 IPS 的资源去判定。我们理解这个“外面”也可以是 C-NGFW 本体内的其他安全业务，它们应该像之前提到的 IPS 那样与防火墙形成紧密的耦合关系，实现自动联动的效果（如思科的“云火墙”解决方案）。

5.3 云数据中心内部安全

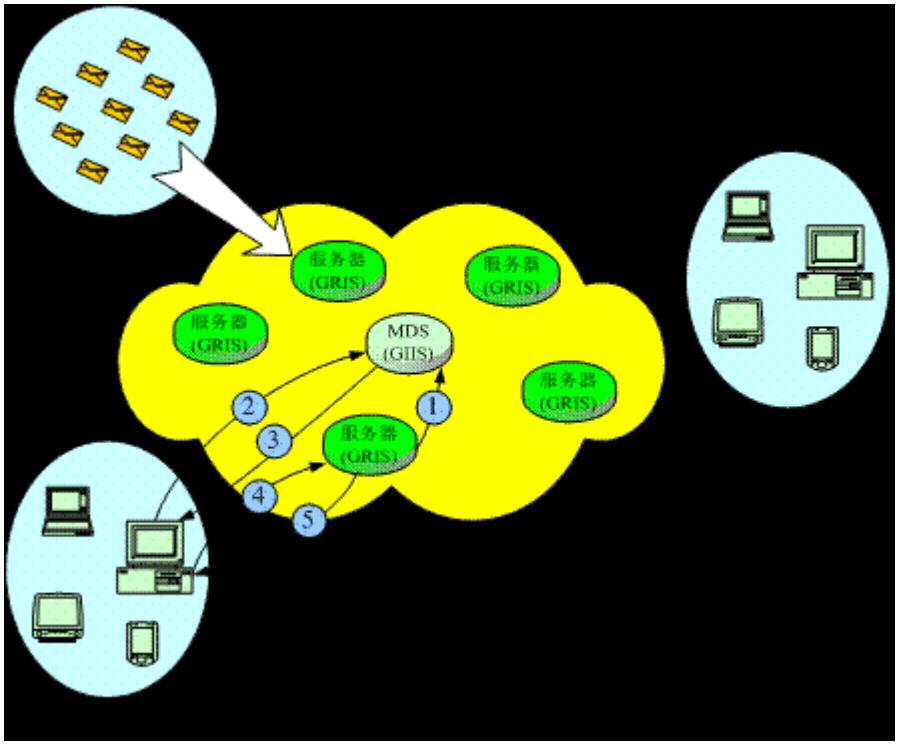
5.3.1 建立分布式云安全体系

在云数据中心内部部署反垃圾邮件、病毒特征库，实时更新特征库，用于给云终端反垃圾邮件和杀毒。 定时对系统（物理主机及虚拟机）进行漏洞扫描，补丁升级等服务。

分布式反垃圾网格思想是国内刘鹏教授提出的观点：

建立一个分布式统计和分布式学习平台，以大规模用户的协同计算来过滤垃圾邮件：首先，我们可以为每一封邮件计算出一个唯一的“指纹”，通过比对“指纹”可以统计同一封邮件的副本数，当副本数达到一定数量，我们就可以判定这封邮 件是垃圾邮件；其次，由于互联网上多台计算机比一台计算机掌握的信息更多，因而可以采用分布式贝叶斯学习算法，在成百上千的客户端机器上实现协同学习过 程，收集、分析并共享最新的信息。

反垃圾邮件网格的系统结构：



上图显示了反垃圾邮件网格的系统结构，它包括反垃圾邮件客户端、过滤服务器和调度服务器，其中，在客户端进行邮件的数字签名计算、贝叶斯学习；过滤服务 器对邮件数字签名及贝叶斯学习成果进行统计和传播；调度服务器根据客户端请求动态地分配过滤服务器。用户如果使用了我们的反垃圾邮件插件，每当收到一封新 邮件时，就会自动生成一个数字签名，发给网格中的一台过滤服务器，该服务器根据全局虚拟数据库，判断该签名的重复出现次数，并返回给客户端。客户端根据这 个次数，就可以知道该邮件的重复发送次数，发送次数越多，它是垃圾邮件的可能性越高。然后再结合分布式贝叶斯算法，就可以比较准确地识别出垃圾邮件，并将 出现假阳性错误的可能性降到接近 0。

利用网格技术的分布式统计功能实现大范围内垃圾邮件的过滤，尚未见到有关文献的报道。它体现了真正 的网格思想，每个加入系统的用户既是服务的对象，也是完

成分布式统计功能的一个信息节点，随着系统规模的不断扩大，系统过滤垃圾邮件的准确性也会随之提 高。用大规模统计方法来过滤垃圾邮件的做法比用人工智能的方法更成熟，它不容易出现误判假阳性的情况，实用性很强；分布式贝叶斯方法是传统贝叶斯方法与网 格环境相结合的产物，它将单点学习过程分布化和协同化，缩短了学习的时间，共享了学习的经验。这两种手段的结合，是在现有主流反垃圾邮件方法的基础上的升 华提高，具有实际应用价值。

综上所述，反垃圾邮件网格通过分布式统计和分布式贝叶斯学习，利用分布互联网里的千百万台主机协同工作来构建一道拦截垃圾邮件的“天网”。该方法可以大大提高垃圾邮件的识别率，同时避免将合法邮件误判为垃圾邮件，有可能使通过技术手段有效解决垃圾邮件问题成为现实。

云平台分布式反病毒也可以采用同样的机制。

5.3.2 云客户端应用介绍

在云终端安装瘦代理程序，启用云软件防火墙，跟云数据中心联动（PANDA，TREND）

5.3.3 云终端接入考虑

云终端以加密方式接入云数据中心（SSH，IPSEC VPN 等等）。

5.3.4 云终端用户数据的备份

云终端用户数据的备份，用户重要数据可以选择加密存储在云端

5.4 分布式认证和日志系统

建立可靠的的认证和计费系统，对外部用户和内部工作人员权限分级控制。

第六章 云安全架构下的产品推荐

如何选择一个好的云安全产品，总结如下：

1. 云安全产品满足分布式数据处理的需要，比如：在云中病毒防护，垃圾邮件过滤等等
2. 云安全产品需要满足虚拟环境下对虚拟机的隔离，起到软件防火墙的作用，对虚拟机内部要能进行病毒扫描和杀毒功能

6.1 HP TippingPoint

HP TippingPoint 保证虚拟安全

惠普推出了虚拟网络安全产品 Secure Virtualization Framework，它由 HP 虚拟控制器(vController)、虚拟防火墙(VFW)、虚拟管理中心 (VMC)和 HP TippingPoint N Series IPS 组成。VFW 能够创建可信域，在虚拟机、集群和应用程序分组中执行分片。vController 和 VFW 位于各个虚拟机管理程序中，可对虚拟机间的流量应用安全策略。 它们共同控制虚拟机之间的通信。vController 还能够将流量发送给入侵防御系统(IPS)。TippingPoint N Series IPS 可以检测流量，并根据 VMC 设置的策略将流量发送回虚拟集群，或者丢弃该流量。

6.3 VMware 云安全方案介绍

VMware 云安全组件包括下列几个方面：

A．个人的数据可以选择加密存储

B. 云终端 PC 安装代理软件

C．在云服务器侧的 Supervisor 安装软件防火墙

D. 在 VM 上安装 VA 软件

E. 日志和报表系统

6.3.1 VMware vShield 系列

VMware vShield 产品线包括 vShield App、vShield Edge 和 vShield Endpoint。VShield Edge 是一个网络和安全网关，它能够保护虚拟数据中心边界。VShield App 支持虚拟机内部通信分片，它能够将应用程序锁定到某些特定端口和必要服务。VShield Endpoint 可以将反病毒功能转移到一个专用的虚拟设备上，从而减少虚拟机中的反病毒客户端。这三个软件产品可以在 VMware 基础架构中独单独部署 或一起部署。

6.3.2 VMsafe

6.3.4 其他产品：

Fortify

Trend Deep Security

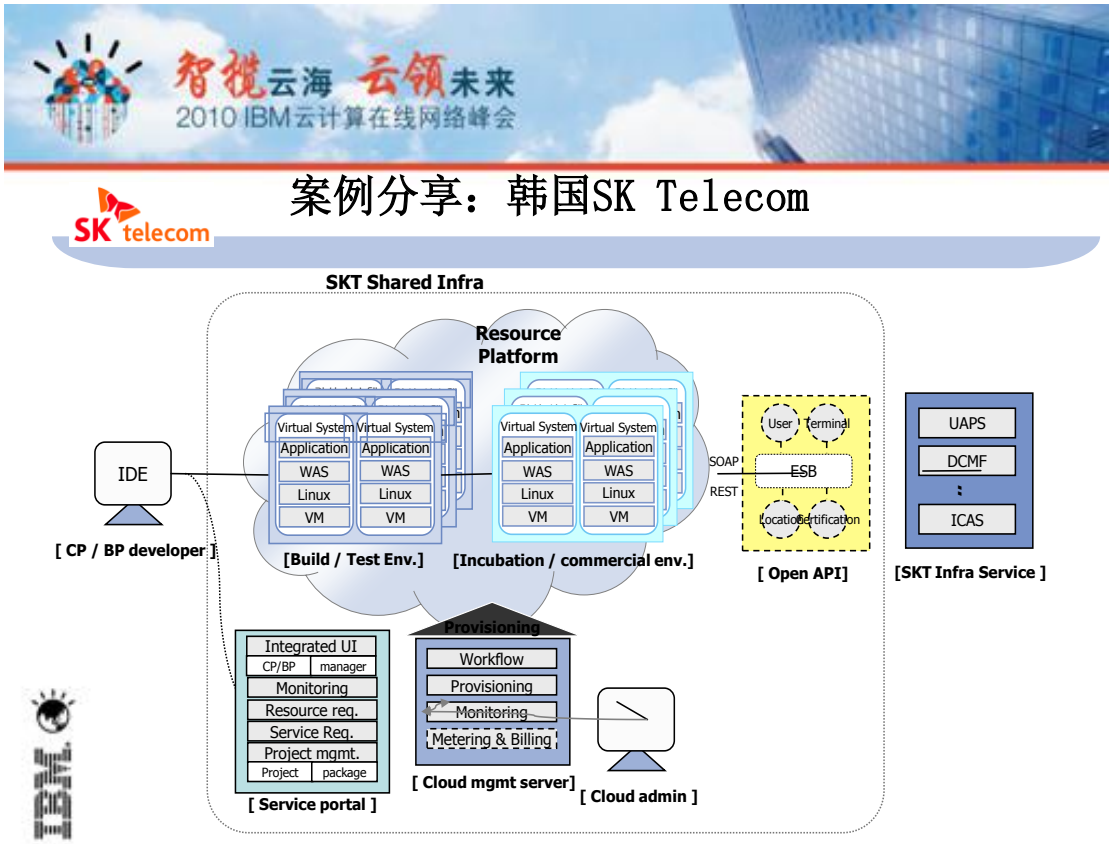
Hytrust

Voyatta NetworkOS

第七章 云计算安全成功部署案例

2011 年底，韩国 SK 电讯联合 MS 公司，通过为服务平台专用防毒软件——‘Forefront Endpoint Protection’设置虚拟平台，从而在让该软件可以单独的在系统 OS 中进行安装　　Symplified 还与亚马逊建立了战略合作关系，并已在亚马逊网络服务成功推出了 Trust Cloud，成为亚马逊云平台唯一的一家身份管理服务提供商。

下图是韩国 SK Telecom 云平台：



最后感言

有了一个写作的目标，就能不断地找到自己的知识结构的弱点，整个写作过程对作者来说受益匪浅，不断总结是自我提升的重要动力。在技术之路上，沿用前人的话：了解得越多，敬畏之心越重，但仍需不断前行，因为即使无法成为引领者，也必将超越原地踏步者。