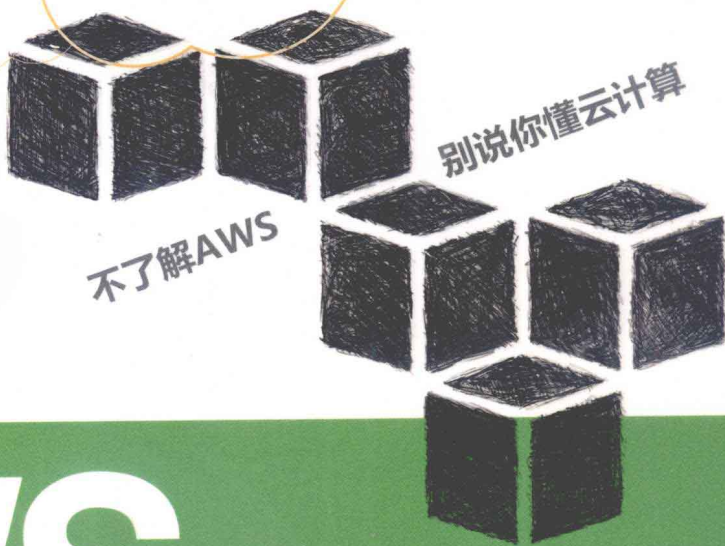


顶尖云端运算服务案例剖析与深入教学用书

解答!

如何保障云端安全? 如何节省云端经费?

如何架构分布式计算? 如何把既有系统直上云端?



AWS

云端企业实战圣经

亚马逊如何构造云端计算

林允溥 著

- 完整剖析与深入讲解亚马逊企业云端计算的图书
- 从入门到进阶、从理论到实践, 带你搞懂亚马逊构造云计算的方法
- 教你如何打造高扩展性、高可用性、安全的云计算系统



清华大学出版社



AWS
云端企业实战圣经
亚马逊如何构造云端计算

林允溥 著

清华大学出版社
北京

本书版权登记号：图字：01-2011-7423

本书为城邦文化事业股份有限公司 PCuSER 出版事业部授权出版发行的中文简体字版本。

内 容 简 介

本书是市场上第一本完整剖析、深入介绍亚马逊云计算服务（Amazon Web Services, AWS）应用的图书，作者林允溥是有多年 AWS 操作经验的专家，擅长构建社群网站和游戏网站的云计算应用系统，本书融入了作者大量的实践经验。

本书以目前最成功的 AWS（亚马逊云计算服务企业）为主题，详细讲解 AWS 的实际应用经验、遇到的各种问题与解决方法，并介绍企业利用 AWS 架设自己的云端数据库、网络应用系统的方法，以及大型网络公司（如 Twitter、Zynga）利用 AWS 的优势，快速更新自己服务的做法。

本书适合云计算架构师、云计算开发人员、云计算应用设计人员，以及想直接使用 AWS 构建自己网站的企业用户参考。

本书封面贴有清华大学出版社防伪标签，无标签者不得销售。

版权所有，侵权必究。侵权举报电话：010-62782989 13701121933

图书在版编目（CIP）数据

AWS 云端企业实战圣经：亚马逊如何构造云端计算/林允溥著. —北京：清华大学出版社，2012.8
ISBN 978-7-302-28746-9

I. ①A… II. ①林… III. ①计算机网络 IV. ①TP393

中国版本图书馆 CIP 数据核字（2012）第 096011 号

责任编辑：夏非彼
封面设计：王 翔
责任校对：闫秀华
责任印制：何 芊

出版发行：清华大学出版社

网 址：<http://www.tup.com.cn>, <http://www.wqbook.com>

地 址：北京清华大学学研大厦 A 座 邮 编：100084

社 总 机：010-62770175

邮 购：010-62786544

投稿与读者服务：010-62776969, c-service@tup.tsinghua.edu.cn

质 量 反 馈：010-62772015, zhiliang@tup.tsinghua.edu.cn

印 刷 者：北京鑫丰华彩印有限公司

装 订 者：三河市金元印装有限公司

经 销：全国新华书店

开 本：190mm×260mm

印 张：24

字 数：614 千字

版 次：2012 年 8 月第 1 版

印 次：2012 年 8 月第 1 次印刷

印 数：1~4000

定 价：55.00 元

推荐序：一本来自云端神人的武功秘笈

我常宣称 Hank 是全台湾第一个开始玩 AWS 的工程师，这样说当然有点夸张，但跟事实可能也相差不多。那是 2006 年的夏天，我和两个朋友在纽约开始创业，Amazon 也刚好宣布他们的 EC2 云端服务器和 S3 云端存储服务开始进入封装测试。我赶紧把申请到的账号给 Hank，请他好好研究一下，然后他认真地钻研了一个多月，等到我们产品正式对外发布时，他已经成功地把 AWS 给的这些积木，组合出一个非常符合我们初期使用的系统架构。

后来发生的事情更有趣，每当我们的网站成长需要系统层面的功能支持时，Amazon 也会刚好开发出相应的东西：当我们需要把处理照片缩图的工作独立出来，Amazon 刚好推出可以专门负责的大型虚拟主机；我们需要播放影片，AWS 开出 CloudFront CDN 服务；我们要服务中国台湾的用户，Amazon 适时增加新加坡的服务器区域。结果从头到尾，我们都没离开 Amazon 的怀抱，而 Hank 也因为一路根据需求不断把 AWS 的新功能纳入我们的架构，最后成为一个对这套云端架构研究得出神入化的大师级人物。

很高兴看到他终于把 4 年多来的心得写成了一本书，让所有有兴趣研究 AWS 的后辈有机会吸收 Hank 身上累积的精华。我想这里面有很多会是创业人，因为对于一个要从 10 万用户成长到 100 万、1000 万，甚至是 1 亿人的网络服务，Amazon 云端平台提供的各种服务有着数不尽的好处和超强的本益比优势。很多人或许不知道，但如果要我说美国 2006 以来的网络产业复兴，最关键的是什么？我会说 AWS 居功厥伟。如果不是 EC2、S3 等服务把系统管理的复杂度大大降低，很多创业团队可能到现在还是卡在规模化的各种问题当中，根本不可能做出这么多可以支持上千万、上亿人使用的网站。

另外，我也希望 Hank 的这本书能起到抛砖引玉的作用，让中国台湾的信息产业了解一流的云端平台到底是什么样子的。AWS 5 年来累积了这么多功能，但没有一个不是从用户的需求出发的。所以 PaaS (Platform as a Service) 的重点不是 Platform，而是 Service，不是把几台机器塞到几个货柜里面，而是去满足创业者、网站开发者的各种需要。也就是因为如此重视服务，Amazon 才能够在北美云端平台达到 96% 的超高市场占有率！这点，我真心地希望还在用制造业思维看云计算的厂商，能够早日有所觉悟。

简单开场到此，重点还是书的内容，所以，请你们好好享用 Hank 为你们精心准备的这本少林武功秘笈，希望你们都能从中练得一身腾云驾雾的好功夫，套一句绝地武士的说法：“愿原力与你同在。”

appWorks 的初创投创办人暨合伙人 林之晨 (Mr. Jamie)

序

在 2006 年，我在一家美国的新创网络公司担任工程师，想要搭上快速成长的社群网络（Social Network Services）的潮流。那时 Facebook 正在快速崛起，把用户从 Myspace 大量地抢过来，网络的生态可以说处在一个瞬息万变的状态。以前可能要 8 年、10 年才会实现数十亿美元的收入（如 Yahoo、Google），到现在可能只要 3、5 年就可以达到了（如 Facebook、Groupon）。所有的变化都是以前不会想到的，以前觉得不可能的事也都一件一件发生了。

要在竞争激烈和快速变化的环境创业，我们适应环境的速度也要非常快才行。在努力的过程中，很多事情就不能单纯地用以前的想法去做，于是其中出现了一个重要的环节，就是“云计算”。

如果你要开一个网站提供服务，在以前，你有几个选择：租用虚拟机，租或买专属机器，然后请数据中心（data center）托管，或是自己搭建一个机房。租用虚拟机一开始似乎是很不错的选择，但是如果网站稍有成长，马上就会遇到性能不佳，以及可伸缩性（elasticity）不好的问题。如果要开始使用专属机器，投入成本就会大增。需要有专门的管理员处理这些硬件，或是和数据中心沟通的事。我们在想，有没有新的方法？

那时“亚马逊网络服务”（Amazon Web Services, AWS）才刚公开没多久，一开始，我和你想的一样：什么？Amazon？不是做网络购物吗？那时我还不知道“云计算”这个名词正要在信息业界流行起来，更不知道这些先驱者从 2002 年就开始建立这些基础设施了。

到 2007 年初，AWS 的文件量就已经非常多了，当然，全部都是英文，这可以说是进入 AWS 云计算的第一个门槛。即使是现在，AWS 仍然以每个月 1~2 次的频率，不断地更新服务，改进功能。以 Google、Microsoft、Rackspace 等其他厂商追不上的速度在前进。

幸好我在最一开始就接触到了 AWS，等我对 AWS 这个全新的东西有了初步认识之后，就对它非常感兴趣，我觉得它很适合我们这个新创公司，而且我相信这也是未来的趋势。当时，我要解决一个存储用户上传照片的问题，最早的做法是直接保存在关系型数据库里，但是这样造成数据库的 I/O 量太大，会拖慢整个数据库。结果我发现 AWS 的 S3 服务非常适合用来解决这个问题，S3 有无限的容量，而且文件有很多副本，所以有非常高的耐用性。

所以我重新架构把照片存储移植到 S3 上，数据库就不会受到照片读取的影响了，也不用计算存储容量来预先增加（购买）硬盘了。

另外，我也规划系统能快速地向外延展（scaling out），并且能够快速地搭建一个测试环境。AWS 的 EC2 就非常适合，所以我就把我们的网站仅有的几台机器，搬上了 AWS 的 EC2 上面。因为我也负责设计系统的架构，所以我可以计划好哪一个部分要如何重构（refactor），并为未来预先做好准备，能够利用云计算的优点，实现高性能、高可扩展性、高可用性的网络服务。通过改进系统架构来适合云计算，可以说是进入 AWS 云计算的第二个门槛。

使用 AWS 帮我们节省了时间，如果虚拟机有问题就丢掉，下达指令就可以再开一个。存储或备份，不用预估和购买容量，也是只要下达指令就可以了。所以在使用工具和管理脚本（scripts）之后，我平常仍然是负责设计和开发网站，但是同时也能够管理日渐增加的机器。

虽然，很可惜地，我们公司并没有像 Facebook 那样疯狂地成长，但是我知道，创业有很多关键，至少在使用 AWS 提供运算能力方面，我觉得是很正确的选择。现在 AWS 已经有二十几种服务了，也有越来越多的人在使用。在 2007 年底，AWS 使用的网络带宽就超过 Amazon 网站本身（Amazon 的网络流量位居世界前 15），AWS 也是 Amazon 的营业额成长最快的项目。这几年“云计算”这个名词也快速地充满媒体版面，成为信息界最火热的名词之一。可以说，现在搭建信息系统，很多人首先考虑的反而是：“系统的这个部分要不要使用云计算？”或是“要使用哪一家云计算服务提供者？”

Google 的执行董事 Eric Schmidt 说过，希望把世界所有的数据都数字化（当然是保存在 Google 了），然后免费提供给所有人使用。所以要取用 Google 的数据，当然要通过因特网了。因为 Google 有这么大量的公开数据和用户，所以 Google 的“不为恶”（Don't be evil）就非常重要了，云计算服务提供者要让人“信任”，可以说是基本要求，毕竟如果有不良记录，就会打破好不容易建立起的信任。

而“亚马逊网络服务”就是目前世界上评价最好、用户最多的云计算服务。本书希望能把这个优秀的云端工具以及作者长期累积的经验心得介绍给大家，提供正确的使用策略，让大家了解云端真正的面貌与魅力。

本书作者 林允溥（Hank Lin）

目 录

第 1 章 谁应该使用云计算

1.1 适应网络未来的云计算.....	2
网络=水、电等民生资源.....	2
云计算就像把发电机交给专责发电厂.....	2
云计算是因为有这样的需求而诞生.....	2
流言终结者：云计算其实不是什么.....	3
1.2 云计算的具体服务内容.....	4
如何定义云计算.....	4
通过云端服务让系统运算升级.....	5
IaaS (Infrastructure as a Service).....	5
PaaS (Platform as a Service).....	6
SaaS (Software as a Service).....	6
1.3 云计算带来的优势竞争力.....	7
传统运算架构的局限.....	7
云计算更有可伸缩性.....	8
云计算更节省成本.....	8
云计算更可用、更持久.....	9
云计算商业性优点快览.....	10
1.4 使用云计算的风险评估.....	10
厂商锁定 (vendor locks in) 考虑.....	10
部署可用性考虑.....	10
网络稳定性考虑.....	11
数据安全性考虑.....	11
数据机密性考虑.....	11
1.5 适合使用云计算的情境.....	12

云计算技术性优点	12
新创公司 (Startup companies)	12
高可扩展性的网络应用	12
大量的运算需求	12
备份与灾害恢复	13
开发与测试	13

第 2 章 云计算领导者 AWS

2.1 AWS 是什么	15
Amazon 与 AWS	15
AWS 的组合式服务概念	15
AWS 特色一览	16
为什么我们尚未善用 AWS	17
2.2 案例：采用 AWS 创造更多利润	17
新兴网站偏爱使用 EC2	17
Zynga 用 AWS 应付用户成长	18
PlayFish 用 AWS 快速推出新游戏	18
Twitter 用 AWS 管理存储空间	18
Reddit 用 AWS 构建数据库	19
MySpace 用 AWS 测试新服务	19
Justin.tv 用 AWS 节省单位成本	19
Smugmug 用 AWS 省下设备费	19
Animoto 用 AWS 应付瞬间超大流量	19
Newsweek 用 AWS 开源节流	19
2.3 如何开始使用 AWS	20
地区和所在地	20
申请 AWS 账号	20
申请个别服务	23
2.4 AWS 上使用的凭证和识别码	26
访问密钥 (Access Keys)	26
X.509 凭证	28

密钥对 (Key Pairs)	29
AWS 账号和密码	29
AWS MFA (Multi-Factor Authentication)	30
AWS 账号识别码和标准化用户识别码	31

第 3 章 AWS 上手必备工具

3.1 AWS 服务快速比较	33
3.2 使用 AWS 的一般注意事项	34
因特网传输收费节约要诀	34
失败重试时的要诀	35
幂等函数避免数据不一致	35
注意服务器时间校定	36
避免 XML 交换格式错误	36
免费使用层级 (AWS Free Usage Tier)	36
AWS 识别及访问管理 (Identify and Access Management)	37
AWS 的访问策略语言 (Access Policy Language, APL)	37
3.3 AWS 图形接口工具	38
AWS Management Console	38
AWS Toolkit for Eclipse	39
S3fox	46
Elasticfox	46
jetS3t	46
AWS 收费计算器	46
3.4 AWS 应用程序接口	46
EC2 API Tools 和 EC2 AMI Tools	47
安装 ec2-api-tools	47
安装 ec2-ami-tools	49
3.5 AWS SDK (开发套件)	50
AWS 已经针对手持设备推出 SDK	50
AWS SDK for Java	50
AWS SDK for .NET	51

AWS SDK for PHP	51
AWS SDK for Android	52
AWS SDK for iOS.....	52
AWS 开发中心	52
s3sync	53
boto	54
jclouds	54
typica	54
cloud tools	55
s3tools	55
3.6 AWS 的其他资源	55
alestic.com	55
AWS 的 blog	55
AWS 的开发者文件	56
其他资源的网址	56

第 4 章 AWS 基础：S3 与云端存储服务

4.1 AWS 的存储功能	58
4.2 一般性的存储功能：S3	59
S3 解决动态数据存储问题	59
S3 的特性	60
容器与对象	61
容器的地区 (region)	63
低备份存储 (Reduced Redundancy Storage)	64
对象版本	65
标头 (headers) 及其他数据	66
访问控制列表 (Access Control List)	67
对象名称浏览 (key listing)	67
多部分上传 (Multipart Upload)	68
日志记录 (logging) 和范围读取 (Range)	68
用 AWS Management Console 开始操作 S3	69

4.3 简单数据库: SimpleDB.....	77
NoSQL 的潮流.....	77
SimpleDB 的特性.....	79
SimpleDB 的相关名词.....	81
再回顾一致性.....	82
SimpleDB 的查询语言.....	83
数值数据.....	85
日期数据.....	86
排序.....	86
计数.....	87
引号 (quoting) 规则.....	87
保留字.....	87
查询的调校.....	88
数据分割.....	89
使用 AWS SDK for Java 操作 SimpleDB.....	89
建立 Domain.....	91
列出 Domain 清单.....	91
查看 Domain 元数据.....	91
读取数据.....	92
新增或更新数据.....	92
条件式新增 (更新) 数据.....	93
查询数据.....	95
删除数据.....	95
条件式删除数据.....	96
批处理更新与删除.....	96
删除 Domain.....	97
实际应用诀窍.....	97
4.4 数据库的另一选择: RDS.....	98
实际的存储需求.....	99
RDS 的概念: DB Instance.....	100
维护与备份.....	105

多所在地部署	106
安全组	107
设置数据库安全组和数据库参数组	109
建立 DB Instance	111
使用与设置 DB Instance	112
备份与恢复	114
建立读取副本	116
从原本的 MySQL 移植到 RDS	116

第 5 章 AWS 核心：EC2 与其相关服务

5.1 什么是 EC2	118
EC2 是 AWS 架构体系中的核心服务	118
从 EC2 服务特色看云计算实质	119
使用 EC2 的优点	119
EC2 开机？亚马逊机器映像文件（AMI）	120
5.2 EC2 虚拟机的基础结构	120
EC2 的 AMI root device 比较	121
EC2 的机器类型比较	122
EC2 机器收费标准比较	122
EC2 新机器类型：集群运算虚拟机	123
EC2 新机器类型：集群运算 GPU 虚拟机	124
32 位或 64 位？这是个大问题	125
5.3 EC2 虚拟机的延伸结构	125
Instance Storage（虚拟机存储）	125
EBS（Elastic Block Store）	126
在 EC2 上使用微软 Windows 系统	127
EC2 云端机器的地区与所在地	128
5.4 EC2 的一些延伸问题与解决	129
EC2 的 IP 地址及 DNS 名称问题与解决	129
解决利用 EC2 传送邮件的需求	131
EC2 的防火墙安全组（security group）	131

元数据 (metadata) 及用户数据 (user-data)	132
EC2 上怎么分配 I/O 资源	133
5.5 EC2 开机操作实战范例	133
登录 AWS Management Console	133
申请 EC2 的 Key Pairs	135
管理安全组	137
开启一台虚拟机	140
进入之前建立的机器	147
第 6 章 AWS 高级：实现 EC2 部署策略	
6.1 使用公开 EBS-backed AMI	152
如何搜索公开的 AMI	152
用 EBS root partition 建立 EBS-backed AMI	155
用挂载的 EBS volume 建立 EBS-backed AMI	156
6.2 建立 S3-backed AMI	160
用来源机器的 root device 建立 S3-backed AMI	161
使用 alestic 的脚本建立 S3-backed AMI	163
使用 loopback 文件建立 S3-backed AMI	164
6.3 AMI 实现疑难问题解决	168
做出无法开机的 AMI 怎么办	168
清理资源	169
虚拟机 (EC2 instance) 的属性修改	169
AMI 的属性修改	174
6.4 AMI 有效实战策略分析	174
一般性 AMI	175
特定性 AMI	176
参考 RightScale 的实现流程	177
6.5 EC2 自动初始化机制	177
EC2 的 user-data	178
使用 ec2-run-user-data	178
使用 runurl	179

管理 EC2 虚拟机常用的工具	181
卷标功能	182

第 7 章 AWS 架构关键 1：组建高可扩展性系统

7.1 高可扩展性和云计算	184
什么是可扩展性 (scalability)	184
可扩展性为什么重要	185
传统模式：向上延展 (scale up)	185
传统模式：向外延展 (scale out)	185
云计算解决延展问题	186
追求高可扩展性	186
常见的高可扩展性架构模式	187
如何实现有效率同步联机	188
7.2 实现负载均衡的做法	189
负载均衡的选择	189
Round robin DNS	190
软件的负载均衡	191
7.3 弹性负载均衡 (ELB)	191
负载均衡器 (Load Balancer) 的概念	192
地区和所在地	193
安装 Elastic Load Balancing API Tools	193
建立一个 HTTP 负载均衡器	195
让负载均衡器分配请求到多个所在地	197
暂停 (disable) 所在地	199
拆掉负载均衡器 (tear down a Load Balancer)	201
建立定时的黏着联机状态 (Sticky session)	201
建立自定义的黏着联机状态 (Sticky session)	203
7.4 自动延展 (Auto Scaling)	205
Auto Scaling 的概念	205
自动延展组 (Auto Scaling Group)	206
触发器 (trigger)	207

重新平衡 (rebalancing)	208
安装 Auto Scaling API Tools.....	209
建立一个自动延展的 EC2 集群	210
建立多所在地自动延展的 EC2 集群	213
合并自动延展组	214
删除自动延展组	215
停止使用自动延展组	215

第 8 章 AWS 架构关键 2: 异步消息构建策略

8.1 什么是异步消息传递.....	218
异步的好处	218
“消息导向中间件”简介	218
AWS 中的消息传递服务.....	220
8.2 AWS 的简单队列服务 (SQS)	220
使用 SQS 的优点	221
使用 SQS 要注意的地方	221
消息队列 Queue	222
可读取 (Visibility) 和读取超时 (Visibility timeout)	223
SQS 里的消息的生命周期.....	224
SQS 的访问控制	224
在 SQS 使用访问权限策略语言的额外限制.....	225
使用 AWS SDK for Java 操作 SQS	225
建立 Queue.....	226
查看 Queue.....	227
查看 Queue 的属性	228
更改 Queue 的属性	229
更改 Queue 的访问权限.....	230
从 Queue 收送消息	232
更改读取超时以及删除消息	234
删除 Queue.....	235
8.3 AWS 的简单通知服务 (SNS)	235

建立主题 (Topic)	236
订阅主题	238
发布消息到主题	240
停止订阅	242
删除主题	242
在 SNS 使用访问权限策略语言的额外限制	243

第 9 章 AWS 架构关键 3: 高可用性的云计算

9.1 为何高可用性重要	246
改进系统架构以适用于云计算	246
云计算有新的策略方法	247
AWS 与传统成本的比较	247
9.2 实现高可用性的基本 AWS 应用	249
使用多重所在地 (multiple availability zones)	249
使用 EIP (Elastic IP Addresses) 实现重定向	249
9.3 EC2 instances 挂掉了如何处理	254
EC2 虚拟机没有回应的检查步骤	254
快速恢复挂掉的 EC2 虚拟机	257
9.4 CloudFront 改进用户体验	261
提供用户最快速的网站使用经验	261
内容传递网络 (CDN)	262
CloudFront 的工作原理	263
文件逾时 (expiration) 的处理策略	266
文件移除 (eviction) 与主动清除	267
发布单位 (distribution)	268
使用自定义来源服务器 (Custom Origins)	268
从 S3 改用 CloudFront	270
用 AWS Management Console 操作 CloudFront	272
文件的 URL	277
访问日志	278
服务流媒体 (streaming media)	279

服务私有内容 (private content)	279
9.5 管理动态 IP 地址的方法	284
使用 EIP (弹性 IP 地址)	285
使用动态 DNS (Dynamic DNS)	285
使用 Hosts 文件	286
9.6 用 Amazon CloudWatch 监视系统健康	286
CloudWatch 的概念	288
使用 CloudWatch	291
安装 CloudWatch API Tools	293
用 mon-list-metrics 列出测量项目	295
用 mon-get-stats 读取统计数据	295

第 10 章 AWS 活用策略：企业云端优化方案

10.1 保护云端数据安全	297
数据传输的问题	297
数据存储加密	298
善用 EC2 的安全组 (security groups)	299
定期更新 OS 的安全性更新	300
10.2 如何善用花在 AWS 上的每块钱	300
使用 EC2 Reserved Instances	301
使用 RDS Reserved 虚拟机	305
使用 Spot Instances 处理大量数据	306
10.3 用分布式运算处理大量数据	312
MapReduce 与 Hadoop	312
云端上的 Hadoop: EMR (Elastic MapReduce)	313
数据安全性	315
Hadoop	315
工作流程 (Job Flow)	317
JSON 配置文件 (JSON Configuration Files)	321
用 AWS Management Console 操作 EMR	322
使用 Elastic MapReduce Ruby Client	328