OpenStack 实战指导手册

OpenStack 实战指导手册

OpenStack 是一个美国国家航空航天局和 Rackspace 合作研发的，以 Apache 许可证授权，并且是一个自由软件和开放源代码项目。OpenStack 是一个云平台管理的项目，它不是一个软件。这个项目由几个主要的组件组合起来完成一些具体的工作。OpenStack 是 IaaS(基础设施即服务)组件，让任何人都可以自行建立和提供云端运算服务。此外，OpenStack 也用作建立防火墙内的“私有云”，提供机构或企业内各部门共享资源。本技术手册我们将侧重介绍 OpenStack 的最新动态，以及如何用 OpenStack 构建云计算，同时我们在最后引入拉美最大在线电子交易网站 MercadoLibre 的实战，看他们如何用 OpenStack 开发云存储业务。

OpenStack 动态

围绕于 Citrix 公司决定将其 CloudStack IaaS 产品源代码与 Apache 合作的媒体炒作，已使业内纷纷有了该公司已放弃 OpenStack 的猜测。由于 CloudStack 是市场上云计算厂商的第二选择，那么此举是否会对 OpenStack 形成真正的威胁呢？另外，现在 Puppet Labs 对 OpenStack 的支持给了云商店更多的理由去选择一个开源的平台。OpenStack 最近也发布了其云 OS 更具扩展性和“可插拔”的版本。

- CloudStack vs.OpenStack：竞争对手还是同盟军？
- OpenStack 与 Puppet Labs 整合引关注
- OpenStack 扩展 Essex 意在吸引大型 IT 部门

用 OpenStack 构建云计算

当你想到 Amazon EC2 的替代品时，诸如 Rackspace、IBM 以及 Savvis 这样的云计算厂商可能会浮现在你的脑海中。但是使用 OpenStack 项目所提供的云计算，IT 团队可以成为他们自己的云计算服务厂商。那么 OpenStack 架构是不是构建 IaaS 云的最佳选择呢？如何用 OpenStack 安全构建私有云？

- DIY 云计算：OpenStack 当积木
- OpenStack 架构是构建 IaaS 云的最佳选择？
- 如何用 OpenStack 安全构建私有云？

OpenStack 实战

OpenStack 是 Apache 服务器许可并由许多更小的项目组成，包括 Nova 计算平台以及一个大规模可扩展冗余存储系统 Swift。使用 OpenStack 的一个方法是使用 Puppet 并安装一个 OpenStack Nova 计算云。另外，迁移至实现授权雇员管理存储器、服务器以及网络资源的私有云计算基础设施并不是一件小事。在实战中我们将介绍拉美电子商务专家 Mercadolibre 公司的实际项目经验。

- 案例：MercadoLibre 用 OpenStack 开发云存储业务
- 如何使用 Puppet 安装 OpenStack Nova 计算云？

CloudStack vs.OpenStack：竞争对手还是同盟军？

围绕于 Citrix 公司上周决定将其 CloudStack 基础设施即服务（IaaS）产品源代码与 Apache Foundation 合作的媒体炒作，已使业内纷纷有了该公司已放弃 OpenStack 的猜测，OpenStack 是一个由 Rackspace 公司和 NASA 共同支持的 IaaS 产品。但是，由于 CloudStack 只是市场上云计算供应商的第二选择，因此此举并未对 OpenStack 形成真正的威胁。

Citrix 公司的产品营销副总裁 Peder Ulander 指出，尽管 Citrix 公司开始支持 CloudStack 的发展，但公司仍将继续与 OpenStack 的合作，“Citrix 公司过去是，现在是，并仍然将会继续是 OpenStack 产品的第五大代码贡献者。在我们使用 OpenStack 代码的同时，我们还支持 CloudStack 中的 OpenStack 对象存储系统，”他说。

Citrix 公司已将 CloudStack 从一个产品转变为一个 Apache2 开源使用许可下的开源项目。Ulander 先生指出，产品与项目之间的区别在于后者更强调社区参与度以及倡导一个更为开放的协作生态系统。

Ovum 公司（一家英国技术咨询公司）的研究主管 Laurent Lachel 表示，Apache Foundation 与 CloudStack 项目的技术合作是建立在中立平等的基础之上。

“通过 CloudStack 与 Apache Foundation 的合作，Citrix 公司将为 CloudStack 项目吸引更多的第三方参与与支持，”他说。

CloudStack 还是 OpenStack：Citrix 公司更多地倾听客户的声音

Citrix 公司决定把重点从 OpenStack 上转移至 CloudStack，是因为客户更欣赏 OpenStack 的成熟度。Rackspace 公司并不总是对 Citrix 公司对 OpenStack 所提出的意见持欢迎的态度。

“我们一直与 OpenStack 共同合作以确保在云计算管理空间中我们与我们客户的兼容性，”Ulander 说。“但不幸的是，在很大程度上是由 Rackspace 来管理和推动 OpenStack 的开发，而 Rackspace 总是在 Citrix 试图作出贡献时很强势地说‘不’”。

Citrix 公司决定通过与 Apache Foundation 的合作，为 CloudStack 启动一个更为开放的社区。“我们希望维持与我们客户合作的长期性和他们的品牌忠诚度，并以一个社区关注的方式推动 CloudStack 的整体发展，”他说。

CloudStack 和 OpenStack 的区别主要在于支持者和信誉，Lachel 说。OpenStack 有 160 个支持者，而 CloudStack 目前有 57 个，其中包括了 Juniper、Intel 以及 Brocade。“其中还有一些同时支持 OpenStack 和 CloudStack 的支持者，尽管 CloudStack 的支持群体较小，但其成熟度更高，并已在更具生产实际的环境中得到了充分验证，”他说。

rPath 公司（Citrix 公司的软件启动合作伙伴）的产品战略副总裁 Shawn Edmondson 说，OpenStack 继续快速发展，而 CloudStack 的发展则更为稳健。

Edmondson 说，从技术和设计方面来说，CloudStack 和 OpenStack 是非常相似的。当 Citrix 公司收购了 CloudStack 的创始者 Cloud.com 之后，众多生产客户也应运而生。行业观察家由此推测，Citrix 公司可能会把重点转向 CloudStack 而不是如之前一样继续全力支持 OpenStack。“但是，从根本上来说，OpenStack 和 CloudStack 都是在以一个非常相似的方式致力于同一个事业，”他说。

CloudStack 与 OpenStack：对于整个行业的意义

Rackspace 公司云计算建设的总经理 Jim Gurry 指出，虽然云计算供应商可以使用 OpenStack 和 CloudStack 作为 IaaS 云计算产品，但是 Citrix 公司认为 CloudStack 是一个具有较好独立主动意识的项目。“Citrix 提出应当有一个第二开源云计算软件项目，”他说。

“我认为该声明是整个云计算市场正在试图弄清楚什么是正确的开源解决方案的一个佐证，”Curry 补充道。“回顾 IT 业的历史我们可以得知，市场总是在围绕着开放技术而发展的，我并不认为最终将会有两个开源云计算解决方案。”

虽然 Citrix 公司正在试图建立其自身的 CloudStack 社区，但是 CloudStack 和 OpenStack 最终可能会融合成为一体，Lachel 说。

“你有两个不同的生态系统，许多人都已尝试创建一个开源云计算项目。即使 CloudStack 并不希望成就自己的系统，但是它仍然计划继续使用 OpenStack 技术，”他说。

Apache 平台将使得这一类型的合作变得更为容易。“通过 Apache Foundation，任何人都可以非常容易地采用这些技术并运行之，”Lachel 说。“与 CloudStack 可以使用 OpenStack 技术一样，OpenStack 同样也可以使用一些 CloudStack 技术。”

（作者：Gina Narcisi　　译者：滕晓龙　来源：TechTarget 中国）

原文链接：http://www.searchcloudcomputing.com.cn/showcontent_60366.htm

OpenStack 与 Puppet Labs 整合引关注

IT 专家还在检验 OpenStack 和它的竞争者，但是 Puppet Labs 对 OpenStack 的支持给了云商店更多的理由去选择一个开源的平台。

OpenStack 最新的增值组件，代号为 Essex，于上周二发布寄希望在云计算和企业市场中吸引大客户。同时，Citrix Systems 为了更好的发展 CloudStack 平台从 OpenStack 分离出来，导致市场上出现了分裂。这两家同时与 Eucalyptus 在开源云的市场中竞争，然而 Amazon Web Services（AWS）和 VMware 仍然占据着主导地位。

Puppet Labs——一个 IT 自动化软件企业，和 OpenStack 陷入冲突因为它正成为一个客户使用的成熟软件，企业的主管们如是说。

“更多的企业不只是谈论 OpenStack，而是在实际生产环境中部署它，包括 Rackspace 基于 Puppet 的公有云” Puppet Labs 的 CEO Luke Kanies 谈到。

早期使用者认为 Puppet 的整合会提升 OpenStack 的吸引力。“我无论如何都要部署 OpenStack，因为我知道我可以用它的 API 写一个 Puppet 模块” Joe Julian——一位 Ed Wyse Beauty Supply 公司的资深系统管理员在邮件中这样述说。“这个整合使它更加吸引人因为它会节省我的部署上时间和金钱。”Puppet 和 OpenStack 之间的整合吸引了一个早就开始测试 CloudStack 的服务提供商的目光。

“我一直都是一个自动化配置的粉丝”华盛顿地区小型教育服务提供商的资深系统管理员 Doug Granzow 如是说“即使是在一个小的规模里我们也喜欢使用它，因为我们清楚服务器都是以同样的方式建立的。”

Granzow——如今使用 Puppet 来管理大约 100 台服务器，认为 Puppet 的介入会让他重新看待 OpenStack，但对于他来说还是太快了。

分析师说，Granzow 和跟他经历相似的人们在未来的一年中是怎么计划的是最近 IT 市场最热门的一个话题。随着 IT 专家评估他们的选项，像 Puppet 这样的工具会有所帮助，根据坐落在 Nashua 的 Illuminata 公司的分析师 Jonathan Eunice 所说。

“假设在未来，OpenStack 没有停止服务同时你想重新托管在 CloudStack，Amazon 或者其他还没出现的环境中，一个像 Puppet 的工具可以帮助你转移，”Eunice 说。相反地“你的选项有限，因为没有一个高级别的自动化建立工具。”

Puppet，有开源版和企业版，允许系统管理员决定他们的基础设施是怎么样的而不用具体指明所有的步骤和流程。Puppet 通过一个资源抽象层实施这些步骤并考虑到速度，可重复系统供应，配置和规模化管理。

OpenStack——最初是服务提供商 Rackspace 和 NASA 合作的产物，提供软件建立模块来建立一个私有云并且包括四个主要服务——计算（Nova）；称为 Keystone 的身份服务；称为 Glance 的图像存储服务；叫做 Swift 的存储对象。

Puppet 和它的合作伙伴 Cisco，Red Hat，Morphlabs 和 eNovance 一起开发的“glue”现在可以用来结合 Puppet 和 OpenStack，从而使四个主要元素的供应和配置自动化，同时拥有快速移动到新版本 OpenStack 的能力。

（作者：Beth Pariseau 译者：薛羽丰 来源：TechTarget 中国）

原文链接：http://www.searchcloudcomputing.com.cn/showcontent_60889.htm

OpenStack 扩展 Essex 意在吸引大型 IT 部门

期望通过宣传吸引大型 IT 部门和高性能计算环境，开源项目 OpenStack 发布了其云 OS 更具扩展性和“可插拔”的版本。

Essex 包含 150 个新功能，这些功能中包括了第一个成熟版本 OpenStack Dashboard，允许管理员通过自助门户访问、准备和自动化基于云的资源；OpenStack Object Storage 其能力紧扣云安全，和文档保存策略保持一致来终止对象；OpenStack Compute，代号 Nova，配合该产品的控制面板和认证功能。

“所有的功能中我们最显著的两个主题就是可扩展性和可插拔性，”Jonathan Bryce 介绍，他是 OpenStack 项目的主席，同时也是 Rackspace Cloud 联合创始人。“这些性能之一就是重构控制面板，允许用户使用基于 Web 的界面管理 OpenStack。你会看到更多的插件（为控制面板设计的），这些插件提供了附加功能，像监控和服务器管理工具等，”Bryce 补充道。

另一个正在准备阶段的项目称之为 Quantum，预期今年秋天在 OpenStack 的 Folsom 中发布，其设计也旨在吸引更大的部门。Quantum 是一个自动化网络管理系统，允许管理员设置虚拟 LAN，而且包含了大量顶层企业的硬件，像思科。

企业 IT 与 OpenStack 的游戏：伺机而动

虽然 OpenStack 加强了其产品的企业级性能，但是一些产业观察者指出这项技术在大型部门之间得到广泛使用还有待观察。他们认为这项技术在未来一两年内还没有为在生产环境中部署做好准备。

“我同使用它的人进行了对话，但是大多数人告诉我他们认为这项技术距离在生产环境中使用要 18 个月，”Bill Claybrook 介绍，他是 New River 市场研究的总裁，“他们认为 OpenStack 还没有为严肃的云计算应用做好准备。”

一些用户也推迟在其部门中部署 OpenStack，但是根据以往的开源产品和技术的经验，部门中看到了其短期价值。

“我看到人们更多的是将 OpenStack 最为战略上的技术来使用，这些人对于开源云感兴趣，而且 IT 部门喜欢一些便宜的东西。OpenStack 应该会变得流行，”Eugene Lee 解释说，他是一家大型银行的高级系统管理员，“我们现在不会开始使用，但是我对于他们新功能的一些方向很感兴趣。”

思杰最近的决定潜在地拖延了 OpenStack 的采用率，思杰是一家顶层云提供商，他们停止了继续支持 OpenStack 基于云的软件。相反思杰计划投入更多的时间和精力到其自己的 CloudStack 产品中，去年思杰收购了 Cloud.com。

“看来思杰已经决定摆脱 OpenStack 群组，将更多地面向其 Cloud.com，”Claybrook 补充道，“很明显，他们对 OpenStack 不寄希望。”

Bryce 表示，Essex 拥有来自 55 个不同公司的 200 为开发者为这个项目贡献代码，这将协助这个项目进入下一个层级。社区也在更多质量保障的时间中构建，从而确保大量技术贡献平稳运行。

“我们决定所做的事情之一就是改变发布周期，因此我们进行了早期功能冻结，这也为我们提供了另外的六周来做更多的测试和集成工作，”Bryce 表示。

除了 OpenStack Object 存储之外，还有很多其他的新存储功能，包括来自初创公司 SolidFire 的一个功能，处理高性能存储矩阵。该公司将其产品同 Essex 集成，允许管理员链接虚拟机（VM）到其存储矩阵。

NetApp 也对其核心产品进行了支持，Bryce 将其看做是提供了一些动力。

“MercadoLibre 是全球第八大电子商务平台，也是 NetApp 的大用户，在 OpenStack 之上运转着 6000 到 7000 之间的虚拟机，”Bryce 补充，“现在该公司和其他的用户可以其 NetApp 资产，直接和 OpenStack 云计算基础架构连接。”

（作者： Ed Scannell 译者：张培颖 来源：TechTarget 中国）

原文链接：http://www.searchcloudcomputing.com.cn/showcontent_60012.htm

DIY 云计算：OpenStack 当积木

当你想到 Amazon EC2 的替代品时，诸如 Rackspace、IBM 以及 Savvis 这样的云计算厂商可能会浮现在你的脑海中。但是使用 OpenStack 项目所提供的云计算，IT 团队可以成为他们自己的云计算服务厂商。构建和维护一个开源私有云计算并不适合每一家公司；但是如果你拥有基础设施和开发人员，这是一个值得努力尝试的选择，而一个良好开端始于 OpenStack。

Rackspace、Citrix、Dell、Cisco 以及微软公司等主要业内厂商都参与了 OpenStack 项目。OpenStack 开发团队致力于一个开放、模块化设计的项目，以支持开放标准和所有主要的虚拟化平台，如 Microsoft Hyper-V、Citrix XenServer、KVM 和 VMware ESX。

共同关注于将企业数据迁移至一个公共云计算的多租户架构，这往往也是构建一个私有堆栈或云计算的动因。OpenStack 项目有一个漏洞管理团队和解决审计与云计算安全性改进的团队，这是一个明确的指示，即安全性是该项目的优先考虑项。虽然以上这些是 OpenStack 的所有积极方面，但最重要的因素是它提供的软件组件。

理解 OpenStack 云计算组件

OpenStack 的架构涉及若干高层次组件，其中包括计算服务器、一个消息队列、一个关系型数据库、网络服务、应用程序编程接口（API）以及一个管理控制台。组件的冗余副本可用于弹性和适用性需求；数据持久保存在分布式数据存储设备中。

一个通过 API 服务器访问的云计算控制器可协调各项云计算服务。一个验证服务器可提供身份验证和授权服务，而一个对象存储组件可实现持久存储服务。

OpenStack 是一个无共享、使用基于高级消息队列协议（AMQP）消息队列并由 RabbitMQ 实现组件通信的系统。云计算控制器对关系型数据库使用一个 Python 工具集——SQLAlchemy，所有任何兼容的关系型数据库都可为云计算控制器提供持久存储。OpenStack 架构提供了三个分别基于子网、DHCP 和 VLAN 的网络配置，它们可允许用户使用虚拟专用网接入项目。

安装和配置 OpenStack

当你准备安装 OpenStack 时，你可以选择使用 ISO 镜像、脚本或一个手工逐步安装方法。该逐步安装方法要求你必须熟悉 git-hub 和 apt-get 工具的使用，以及对 MySQL 或 POstgresSQL 等关系型数据库进行配置等工作。

一旦你安装了该软件，你将需要使用一系列配置文件对 OpenStack 进行配置，其中最重要的配置文件是 nova.conf. (Nova 意为 OpenStack 中的计算服务)。在该配置文件中，你需要对虚拟化、网络、关系型数据库、镜像服务器信息、目录服务以及 API 连接参数指定相关设置。你还需要配置身份服务作为基础，并定义用户和角色。

安装 OpenStack 的存储服务或 Swift 作为一个单独的组件。请记得：OpenStack 开发人员建议为生产集群设置至少五个节点。一个可选组件——OpenStack 控制台可为 OpenStack API 提供一个网络接口。

当构建 OpenStack 云计算时无错误

如果你认为 OpenStack 中有大量可移动部分，你猜对了。每次你安装一个组件或配置一个设置时，你都有可能引入错误。设置配置参数是一个常见的问题源；管理员们常常会错误配置网络设置、关闭计算服务器上的后台程序或在系统上运行错误类型的镜像。

其他问题会发生在实例中；例如一个处于停滞状态的实例可能是由于一个支持虚拟机、磁盘、内核或 RAMDisk 的丢失或损坏文件引起的。通过设置供调试使用的日志记录选项，你可能可以收集有关问题过程的足够细节以找出根源。

OpenStack 云计算系统也有一系列复杂的依赖关系。该文档提供了对特定组件安装所需包以及如何通过使用 apt-get 这样的包管理工具箱来获得它们的详细说明。遵循该文档的指示将有助于减少创造无法满足依赖关系而带来的风险。

运行一个私有云计算要求付出大量的精力、时间以及对基础设施有着极为透彻的了解。OpenStack 是一个具有良好支持的开源云计算项目，它可提供一个配有完整计算、存储、镜像以及身份管理等组件的强大平台。

（作者：Dan Sullivan　译者：滕晓龙　来源：TechTarget 中国）

原文链接：http://www.searchcloudcomputing.com.cn/showcontent_59673.htm

OpenStack 架构是构建 IaaS 云的最佳选择？

OpenStack 已引起了业内众多眼球的关注，这是一个承诺为建设公共云计算和私有云计算建立通用基础的开源项目。如果实现了 OpenStack 的大规模实施，其架构就可以进一步促进混合云计算的实施、有助于云计算联盟的建立以及对高效云计算运行相关的一些关键配置任务的支持。

它甚至可以改变我们看待云计算与网络之间关系的看法。但是，如同其他众多技术一样，OpenStack 是否存在着被过度炒作的风险呢？这个问题可能是云计算中最为关键的问题了，同时它也是难以给出合适回答的。

OpenStack 架构：一个具有竞争力的先天不足？

OpenStack 最初是一个由 NASA 和 Rackspace 公司共同开发的项目，它旨在提供一个可以在成熟商业硬件产品上运行的云计算框架。OpenStack 架构囊括了云计算中的各类模式，其中包括资源分配、机器-镜像配准与控制，以及数据存储等。目前，该项目已有超过 150 家以上的组织参与其中，这使得它成为创建基础设施即服务（IaaS）环境的最流行软件工具。

但是，作为一个商业化的云计算平台，其用户数量排名仍然落后于 Amazon 公司的弹性云计算（EC2），而微软公司的 Azure 平台也是一个强大的竞争对手。它的 IaaS 关注焦点、它所受到的广泛业界支持以及它所面临的激烈竞争都成为了 OpenStack 变得强大或弱小的重要因素。

IaaS 是云计算的最基本形式，基本上它所提供的虚拟裸机就是一台服务器。因为它只是更换服务器和可能的本地存储器，所以，与平台即服务（PaaS）和软件

即服务（SaaS）相比，IaaS 的相对用户成本较高而与之相关的利润则较低。虽然潜在的云计算供应商和用户可以在 IaaS 之上构建 PaaS 和 SaaS，但是很难衡量这些更为复杂配置的效益。但是，如果运营商们关注于 OpenStack IaaS，他们可能会一跃踏上由数百竞争对手所提供的平台之上，这就可能将他们置于无法（除通过定价以外）区分他们云计算服务的窘境。

而反对意见是，OpenStack 架构实际上可以有助于服务供应商通过为 IaaS 提供所有的基本基础而区分他们的云计算产品，让供应商专注于其他的功能和增强功能。OpenStack 是开源的、易于集成的且已与众多有趣项目相关的，这些特点都促使其基本功能逐步提升。事实上，这些项目中有许多都拥有着交集，这一点恰恰促成了以特定市场机遇为目标各种各样基于 OpenStack 部署，从而为供应商们提供了区分各自产品与竞争对手产品的广阔空间。一个云计算供应商的最大竞争对手并不是另一个基于 OpenStack 的供应商。而是 Amazon 公司。

与其他诸如 Eucalyptus 或 Nebula 等 IaaS 云计算工具不同，OpenStack 架构还未关注 EC2 的兼容性。OpenStack 计算所使用的应用程序编程接口（API）不同于 EC2 模式，但是 OpenStack 社区承诺保持现有应用程序的 EC2 兼容性。虽然，它可能仍然可以在运行在 EC2 的 OpenStack 上构建应用程序，反之亦然，但是它仍然可能构建与 EC2 完全不兼容的 OpenStack 基于 IaaS 应用程序。

在镜像管理和存储方面，这两个平台之间存在着明显的差异。这就意味着两件事情：它可能更难以使用 EC2 和 OpenStack 云计算来支持客户，而采用 OpenStack 的云计算供应商不能指望把 EC2 用户迁往他们的服务而不对应用程序或他们自己的环境做出改变。

DevOps 与 OpenStack：路在何处？

从技术完整性的角度来说，OpenStack 架构还存在着其他的问题。

可以扩展 OpenStack 资源控制的基本机制，以便于支持“容器配置”模型，在这样的模型中应用程序与容器及其规则相关。其中的规则包括如何为给定的应用程序分配资源以及在应用程序在服务时如何解决问题。这些项目都属于一个名为 DevOps 的通用目录，该目录定义了如何统一云计算应用程序开发、云计算配置与应用程序部署。在简单实用虚拟机以取代专用内部服务器的 IaaS 云计算中，DevOps 并不是关键，但是，如果一个 IaaS 产品将用于构建特定云计算应用程序，那么它就是绝对至关重要的。

IBM 公司近期对使用云计算重整业务流程（而不仅仅是外包现有应用程序）重要性的研究表明，云计算的未来可能在于它如何支持我们今天在数据中心中无法实现的工作，而不是简单地更新重复我们已完成的工作。这就意味着编写新的云计算应用程序。如果这样做了，那么如 DevOps（促进软件元素的组件化和业务流程）的现代软件实践必须为这些元素提供一个在云计算中互相寻找对方的机制。如果一个 IaaS 云计算被用于托管 PaaS 或 SaaS 服务，那么具有同一应用程序灵活性是必不可少的。这里还有一个问题：OpenStack 的 DevOps 是不完整的，除非经过精心梳理，否则 PaaS、SaaS 或特定云计算应用程序就无法在 OpenStack 架构上实现轻松实施。

有人认为，OpenStack 的所有问题是 OpenStack 所独有的问题，当然这样的说法并不完全公平。事实上，其中大多数问题都与云计算服务的 IaaS 模式相关。但现在，OpenStack 应用可能是 IaaS 市场中唯一一个服务选择，但是从长期来说它可能并不是供应商的最佳服务选择。在考虑决策 OpenStack 架构是构建公共云计算基础设施最佳框架之前，所有这些都需要慎重考虑。

（作者：Tom Nolle　译者：滕晓龙　来源：TechTarget 中国）

原文链接：http://www.searchcloudcomputing.com.cn/showcontent_61885.htm

如何用 OpenStack 安全构建私有云？

如果你已经决定投入并构建你自己的云，那么恭喜你！现在不是仅仅构建安全的图片、锁定实例并管理你的数据，你也要确保运行的整个基础架构的安全。

有人常常认为运行私有云来解决与公有提供商，像亚马逊和 Rackspace 相关的安全问题。但是仅仅因为你的源在防火墙之后并不意味着安全问题逐渐消失。你可能不必担心多租户的风险，但是先要对确保整个的物理硬件的安全负责。

在使用像 OpenStack 这样的较为年轻的平台的时候尤其困难，这个平台仅仅才两年而且文档不健全。我个人学习了一些 OpenStack 的内容，在这篇技巧中，我讲讨论下如何使用 OpenStack 构建私有云，基于我的研究以及一些亲身体验的测试，会覆盖一些安全部署的步骤。

OpenStack：如何构建私有云

第一步是设置正确的硬件和网络环境。尽管 OpenStack 允许我们在一个单一的平面网络上部署一切，从安全的角度来看并不安全。取决于你所使用的管理程序以及虚拟网络接口，它会允许 guest 虚拟机嗅探管理流量。我建议你至少使用两个网络：一个用来管理流量，一个用来进行虚拟机之间的对话。这意味着所有的云计算结点中你需要两个网卡（一个运行实例）和网络管理者。这些应该运行在不同的 IP 范围中。

计算结点和实例的网络也需要支持 VLAN 标记，因为这是在“项目”之间隔绝流量所使用的机制。一个项目等价于你的亚马逊 EC2 账户，除了你不能按照你所希望的数目创建和分配之外。每一个项目都有自己的管理员和用户，在既定项目中的所有实例可以彼此通信。通过指派每一个项目自己的 VLAN 以及内部和外部的 IT 地址池来执行。

一旦硬件和网络设置好，下一步就是确定在哪里部署所有的 OpenStack 组件。标准部署颖有一个控制器和一系列计算结点。控制器运行消息服务器，数据库和其他的组件来编排云，同时计算几点运行实例。但是你也可以分解控制器为地理的部分，从而改善性能，像把 MySQL 放在不同的物理盒中。对于安全而言，最关键的是确保每一部分都安装在安全的主机上，你只需要将其附加在网络上，让云运转即可。

只有两部分需要暴露给外面的世界（即使那只是你的企业网络）：API 服务器/Web 控制台（如果开启）和网络管理者。这些服务器需要过硬，你甚至可以使用第三方网络接口来隔离后端管理用户连接产生的流量。

如果你遵循默认安装说明书，可能这些部分并不如他们应该的那样安全。下面是一些具体的改变：

* MySQL 服务器使用指定的用户账户，不是根 MySQL 管理账户。这个账户和密码将会暴露在每一个云结点上，即使使用基于证书的认证，因此所有结点需要访问这个数据库服务器。

* MySQL 配置文件中，限制访问服务器，OpenStack 用户账户为唯一授权 IP 地址。

* 移除任何不需要的 OS 组件并确保你所设置的服务器只支持通过 SSH 的基于密钥的登陆。

* 默认 MySQL 和 RabbitMQ（消息服务器）流量不加密。如果你隔离了管理网络和坚固的主机，这就不应该是一个很糟糕的风险。如果你的云网络易于嗅探（例如，它和其他服务器共享网络），你需要加密流量。你可以使用 OpenSSL 来进行 MySQL 和 RabbitMQ 处理。（我个人还没进行测试，因此配置可能有点难。）

下一步，记住如果你支持 Web 管理控制台，默认不适用 SSL。这要比其他的管理组件更成问题，因为通常是外部访问。你会最清楚希望使用 Apache 和 SSL 来配置。

这些仅仅是你开始做的一些基础。我们已经略过了像配置 CloudPipe（专用 VPN 开发者可以用它访问项目实例），管理开发者证书，构建安全图片或者控制管理程序，但是这些步骤将会协助你开始项目，而且是一种安全的基础架构。

（作者：Rich Mogull　　译者：张培颖　来源：TechTarget 中国）

原文链接：http://www.searchcloudcomputing.com.cn/showcontent_59217.htm

案例：MercadoLibre 用 OpenStack 开发云存储业务

迁移至实现授权雇员管理存储器、服务器以及网络资源的私有云计算基础设施并不是一件小事。本文中，我们将介绍拉美电子商务专家 Mercadolibre 公司。

位于阿根廷部布宜诺斯艾利斯的公司（该公司在 14 个国家提供了类似于 eBay 公司的服务，并将 eBay 公司作为其投资人之一）在过去一年中一直致力于公司自己的开源云计算存储项目——这是一个使用由 Rackspace 托管公司和 NASA 建立的 OpenStack 社区提供的开源软件（OSS）的私有云计算基础设施。

该项目团队可能再需要一年或更多的时间来微调和完成基础设施即服务（IaaS）模式的转换工作，希望能够实现更快的 IT 资源交付并帮助公司的开发人员为其网站更快地进行功能与应用程序更新。

对于我们来说，最困难的事情是改变整个公司已习惯的业务流程；例如，请求服务器、运行一个应用程序或允许基于品质保证的测试工作，“MercadoLibre 公司的高级基础设施工程师 Leandro Reox 说。

直至去年年初的时候，IT 基础设施团队已经认识到，它根本无法简单快速的提供服务器以满足公司开发人员和内部客户的要求 。规模扩张问题还涉及到基于 NFS 的 NetApp FAS6280 和 FAS6080。

实施一个基于服务的私有云计算将产生近乎实时的影响。在实施私有云计算之前，系统管理员们可在 18 月的时间里交付近 2000 台虚拟机。自从去年八月提供自助部署选项以来，基础设施团队坐观虚拟机数量增至 6000 台，Reox 说。

但是，虚拟机交付只是众多问题拼图中的一块。当 MercadoLibre 公司实施其开源云计算存储项目时， 它希望涉及其基础设施的每个部分，其中包括存储系统和数据库，以及通过私有云计算和公共云计算资源实现的服务。其视野也扩展到使用应用程序，或至少包括他们的前端，以便于在那些由 Amazon.com 或 Rackspace 公司运行的公共云计算上运行。

仅仅为了一次营销活动，我们的业务增加就如同一个怪物一般，因此我们必须准备自动扩展规模，而应用程序架构的改变也赋予了我们以稳定的方式更快扩展规模的能力，“Reox 说。

新方法是存储基础设施发展的必然结果。为了弥补网络附加存储（NAS）和网络文件系统（NFS）规模扩展的限制，项目团队决定为其网站及其他静态信息的客户提供产品实施更具扩展能力的对象存储。他们还计划通过 OpenStack 系统上的冗余对象复制从根本上实现自动备份。

Reox 表示 MercadoLibre 公司出于其主要数据库速度和可靠性的考虑，将对其高端的 NetApp FAS6280s 和 FAS6080s 进行从文件到块存储的转换。团队采购 NetApp FAS3270s 用于虚拟机和 MySQL 数据库的块存储。开发人员可以编写批处理作业，以实现从 NetApp 到 OpenStack 对象存储的任意数据转换。

为了让应用程序能够在公共云计算上运行，开发人员将需要把应用程序从他们用于数据访问的 NAS 系统中分离出来。这也就意味着，重写部分代码可实现通过 API 调用的对象存储系统数据访问。

到目前为止，MercadoLibre 公司使用 Amazon 的公共云计算只测试了数量有限的前端网络和应用程序服务器。开发人员将在未来几个月的时间里主要从事重新编写代码的工作，Reox 说。

在新模式下，为访问者提供页面访问的前端网络服务器可以在公共云计算上运行，但是通过由互联网 URL 发布的外部 API，他们就可能访问任何他们所需的数据。而运行虚拟机和存储数据的 URL 则指向私有云计算。

“我们可以在这个星球的任意位置只使用一个 HTTP API 调用就检索信息，”Reox 说。

虽然其优势可能巨大，但是其实现过程可能并不顺利。例如，OpenStack 的早期发布期间相关文档极度缺乏，MercadoLibre 公司的项目团队不得不深入研究代码以便于开发一个自定义 API 来完成 OpenStack 服务器集群工作负载平衡的功能。

Reox 表示，目前相关文档已得到了改善；一个 OpenStack 社区项目正在更新文档。不幸的是，其改善的速度并不能满足部分用户。

OpenStack 证明挑战

位于美国的 Dragon Slayer 咨询公司总裁 Marc Staimer 说，他知道一家金融服务公司在四个月之后就结束了与 OpenStack 的合作，而另一家关注媒体和娱乐的公司则对 OpenStac 的文件大小限制感到不满。

“他们认为，‘我们可以免费提供。’然后，他们在了解之后就变得非常失望，“Staimer 说。“实施 OpenStack 是非常困难的。所有跟我谈论过的人都认为，你需要一些非常有才华的人来来使其高效运行。

MercadoLibre 公司有四个前系统管理员/IT 基础设施工作人员开始其私有云计算工作，目前项目中有五人。OpenStack 帮助他们提出请求，请他们提供鼎立支持并为开源软件做出贡献。

“我们热爱开源，”Reox 说。

MercadoLibre 公司的高级基础设施工程师 Alejandro Comisario 说，存储管理员们应当在他们的工作中为重要变更做好准备，甚至学习一些编程技巧，同时开始用新方法思考存储规模扩展问题。

“还有大量的工作要做，但是实际上它是非常拥去，”Comisario 说。“你将会觉得存储的每个块实际上是被更有效地使用，并被更为广泛地提供给每个人。最终，有效负载要多于其付出。”

到目前为止，MercadoLibre 的项目团队已实施了 OpenStack 软件平台的五个组成部分：“Nova”计算、“Nova”容量块存储、“Swift”对象存储、“Glance”镜像服务以及“Keystone”身份认证服务。（引号中的名称代表了代码名称。）

在 2011 年 7 月，团队开始着手 Nova 计算软件的工作以便于为公司提供和管理虚拟机，这些虚拟机都在开源 XenServer 上运行，而 Nova 容量软件可使虚拟机块存储持久。Reox 说，这两个组成部分的服务在 8 月份都向内部客户开放用以进行自助供应。

而开发团队在 12 月开放给开发人员使用的 OpenStack 对象存储服务使用价格低廉的商品服务器集群以便于存储 PB 级的一般静态数据。

“MercadoLibre 公司遵循 eBay 模式，并拥有大量客户上传的临时图像文件。这简直就是为 Swift 量身定做的完美应用案例。对象存储是专为大批量相对较小文件而设计的，“位于波士顿云计算技术伙伴公司（CloudTP）的高级云计算架构师 Beth Cohen 说。CloudTP 是 Rackspace 的合作伙伴，旨在帮助公司用户实施开源云计算解决方案，如基于 OpenStack 的 Rackspace 云计算：私有版。

OpenStack Glance 镜像服务存储 MercadoLibre 公司已定义的虚拟机镜像。开发人员查看现有镜像并选择其中最合适的，例如为 MySQL 数据选择一个 Red Hat Linux 镜像，或为 Apache Tomcat 服务器选择一个 Ubuntu 镜像。

MercadoLibre 公司还在去年年底花费了若干天用于实施 Keystone 身份认证服务，该服务处理访问资源与服务的认证和用户权限任务。例如，一个用户可能被允许访问对象存储服务，而不被允许创建一个虚拟服务器实例。

Comisario 表示，MercadoLibre 公司自从启动 OpenStack 以来从未经历过重大中断事件。但是他知道，如果代理服务器上的身份验证服务发生故障，存储访问被中断，那么公司需要对此做出快速响应。

“你知道的，它总是会在某个时候发生故障的”，他说。“你必须尽可能快地进行恢复。”

2012 年 MercadoLibre 公司计划在惠普公司服务器完全到位后把 Swift 对象存储进行全面投产。项目团队还计划使用 OpenStack 量子网络管理器和 Melange IP 地址管理实现网络层的虚拟化。

目前，MercadoLibre 公司使用光纤通道连接其 NetApp 设备和核心交换机，以及边缘交换机和核心交换机。在它的数据库服务器和交换机之间，它还拥有 10G 的以太网连接，而在动态链接聚合模式中是 2Gbps。

“也许在 2013 年年底，我们有望实现我们的私有云计算。我们正在快速而全力以赴地为这个目标而工作着，“Comisario 说。“但是，我们为我们今天所取得的成绩而感到由衷的高兴。”

（作者：Carol Sliwa　译者：滕晓龙　来源：TechTarget 中国）

原文链接：http://www.searchcloudcomputing.com.cn/showcontent_61979.htm

如何使用 Puppet 安装 OpenStack Nova 计算云？

OpenStack 从 Rackpace Cloud 和 NASA 的合作中出现，它提供运行在标准化硬件上的云计算服务。现在一个有超过 60 家公司的社团正在研发它。OpenStack 是 Apache 服务器许可并由许多更小的项目组成，包括 Nova 计算平台以及一个大规模可扩展冗余存储系统 Swift。

使用 OpenStack 的一个方法是使用 Puppet 并安装一个 OpenStack Nova 计算云，这就是我们将在这篇文章中讲述的内容。Nova 计算组件大体上等效于 Amazon EC2 的功能。它允许你使用包括 AMI 镜像在内的镜像文件来部署虚拟机以及管理这些已部署的实例。

首先，我们将要构建一个 Ubuntu 11.04 主机（Ubuntu Natty 的 ISO 文件）。最好是选择一个物理主机而不是一个虚拟机，这不仅是因为性能原因，还因为在一个虚拟化内部进行虚拟化会引起不可预知的结果。如果你想要运行许多不同的镜像，那么你将需要大量硬盘空间，至少 10 到 20G。

接下来，你需要在主机上安装 Puppet 和 Git：

```
$ sudo apt-get install ruby rubygems git
$ sudo gem install puppet
```

Nova 需要通过一个 PPA 或者称为个人软件包存档来完成安装，它是一个包含 Nova 计算组件当前开发版本的软件包储存库。这是必需的，因为 Nova 处在一个过度的研发状态，同时最近打包的发行版本还不存在。

```
$ sudo apt-get install -y python-software-properties
$ sudo add-apt-repository ppa:nova-core/trunk
```

接着你需要更新 APT 储存库来获得新的 PPA 的详细信息：

```
$ sudo apt-get update
```

此时，使用 Git 从 OpenStack 处下载 Puppet Lab OpenStack 组件。

```
$ cd ~ && git clone  -recurse
git://github.com/puppetlabs/puppetlabs-openstack.git
```

把所下载的组件复制到 Puppet 组件路径：

```
$ sudo cp -R ~/puppetlabs-openstack/modules/* /etc/puppet/
```

现在你拥有了在主机上安装 Nova 所需的所有东西。想要进行实际的安装，你需要在主机上触发运行一个本地的 Puppet。

```
$ sudo puppet apply --verbose ~/puppetlabs-openstack/manifests/all.pp
```

这将会运行 all.pp Puppet 清单，它将会安装并配置 Nova 的所有组件以及其支持包和必备条件。

一旦 Puppet 已运行完成（它可能会花一些时间，因为它必须下载许多程序包），然后你需要添加一些 AMI 格式的镜像。

```
$ cd /tmp
$ mkdir lucid_ami && cd lucid_ami
$ wget -q -O - http://173.203.107.207/ubuntu-lucid.tar | tar xSv
```

这会下载并解压一个包括我们可以用来创建实例的明晰示例 Ubuntu 镜像在内的压缩文件。然后，你将把这些镜像文件，包括一个内存盘、一个内核以及一个操作系统镜像文件，添加到一个称为 Glance 的服务中，这个服务是一个用于发现、记录并检索镜像的 OpenStack 服务。

首先添加内存盘和内核。

```
$ glance add name=ramdisk disk_format=ari container_format=ari
is_public=True < initrd.img-2.6.32-23-server
$ glance add name=kernel disk_format=aki container_format=aki
is_public=True < vmlinuz-2.6.32-23-server
```

然后你可以列出已经被添加的镜像：

```
$ glance index
```

发现 2 个公开的镜像...

```
编号                 名称                 磁盘格式             容器格式
大小
---------- ---------------- ---------------- ---------------- -------
-------
2            kernel               aki              aki
4099360
1            ramdisk              ari              ari
7988037
```

你应该看到了你的内存盘镜像#1 以及我们的内核#2。然后你可以连同我们明晰的操作系统镜像一起使用它们并也把它添加进去：

```
$ glance add name=lucid_ami disk_format=ami container_format=ami
is_public=True ramdisk_id=1 kernel_id=2 < ubuntu-lucid.img
```

然后再次列出镜像文件，发现你现在拥有镜像#3：一个你将其作为一个虚拟实例推出的明晰的 Ubuntu AMI。

```
$ glance index
```

发现 3 个公开的镜像文件...

```
编号          名称          磁盘格式          容器格式          大小
-------- ---------- ---------------- ---------------- --------------
```

3	lucid_ami	ami	ami	524288000
2	kernel	aki	aki	4099360
1	ramdisk	ari	ari	7988037

你也可以添加其它的多种格式的镜像到 Glance。

接下来，你需要通过运行一些 Nova 子命令来设置你到 Nova 的访问权限和身份验证，这会产生一个密钥对，用来验证我们的 Nova 实例（类似于使用 Amazon AWS 的密钥对）。这些相同的命令还会创建一个 Bash 脚本，用来设置合适的环境变量来验证 Nova。

```
$ cd ~
$ sudo nova-manage project zipfile nova novaadmin
```

现在，你应该拥有了一个包含密钥对和 Bash 脚本在内的被称为 nova.zip 的压缩文件，它需要解压：

```
$ unzip nova.zip
```

运行 Bash 脚本来填充我们的身份认证和环境变量。在你可以通过一个命令行会话与 Nova 进行交互之前，你需要运行这个脚本，或者把它的运行作为登录的一部分。

```
$ source novarc
```

最后，添加你的密钥对，调用配对的 openstack：

```
$ euca-add-keypair openstack > ~/cert.pem
```

现在，你可以使用这个密钥对来运行一个实例了。寻找一个镜像来运行：

```
$ nova image-list
+----+-----------+--------+
| 编号 |    名称    | 状态    |
+----+-----------+--------+
| 1  | ramdisk   | ACTIVE |
| 2  | kernel    | ACTIVE |
| 3  | lucid_ami | ACTIVE |
+----+-----------+--------+
```

然后寻找这个镜像的一个特色来运行。特色描述了你将要运行的这个镜像的大小和类型。在 Amazon AWS 世界，这是一个小中、大实例间的不同之处。你将会发现该功能与 Amazon EC2 相似。

```
$ nova flavor-list
+----+-----------+-----------+------+----------+-------+------------+---
-------+
| ID |    Name   | Memory_MB | Swap | Local_GB | VCPUs | RXTX_Quota |
RXTX_Cap |
+----+-----------+-----------+------+----------+-------+------------+---
-------+
```

```
| 1  | m1.tiny   | 512       |      | 0         |      |           |
|
| 2  | m1.small  | 2048      |      | 20        |      |           |
|
| 3  | m1.medium | 4096      |      | 40        |      |           |
|
| 4  | m1.large  | 8192      |      | 80        |      |           |
|
| 5  | m1.xlarge | 16384     |      | 160       |      |           |
|
+----+-----------+-----------+------+-----------+-------+-----------+---
-------+
```

在这个例子中，我们将选择运行一个小特色的 ami-00000003 镜像实例，就是你刚刚添加的明晰 Ubuntu 镜像，并使用 openstack 密钥对：

```
$ euca-run-instances ami-00000003 -k openstack -t m1.tiny
```

启动和配置实例将会花费好几分钟的时间，同时你可以使用以下命令来跟踪它的状态：

```
$ euca-describe-instances
i-00000001      ami-00000003 11.0.0.2          11.0.0.2
building            m1.tiny
```

这里你可以看到该实例已经启动并且已为其分配了一个 IP 地址：11.0.0.2。有了这个 IP 地址和你的密钥对，你现在就可以通过 SSH 连接到这个新的实例。

```
$ ssh -i ~/cert.pem root@11.0.0.2
```

当你登录到这个新的实例以后，你就可以设置它，在它上面部署应用程序以及使用它直到你不再需要它为止（你可以通过 euca-terminate-instance 命令来终止这个实例）。你也可以生成其它实例并使自己可以运行你自身的开源云。

OpenStack 才刚刚起步，同时，包括身份验证和数据库服务等在内的许多附加的项目也正在进行中，而且现有的组件每天都在扩展和更新。如果你想要更深层次的了解 OpenStack，那么你可以参考一些文档，或者看看邮件列表，在那里你可以得到帮助或者参与研发。

（作者：James Turnbull 译者：Dan 来源：TechTarget 中国）

原文链接： *http://www.searchsv.com.cn/showcontent_50554.htm*