第194讲 | 刘俊强：2019年云计算趋势对技术人员的影响

2019-03-27 腾讯云资深架构师刘俊强

技术领导力300讲 进入课程 >

讲述：刘飞

时长 09:57 大小 9.12M

你好，我是腾讯云资深架构师刘俊强，之前提到 2019 年的云计算趋势主要体现在五大方面，分别是：云服务市场将继续增长强劲；混合云和多云（Poly-Cloud）将逐渐成为主流；自动化将不可或缺；合规性和安全性将受到重视；云服务将依然是新技术的最佳试验地。

那么，这样的趋势会对技术人员产生什么影响呢，技术人员又该如何应对这样的趋势变化呢？

一个普遍的共识是，云计算优先概念将在接下来的几年内被普遍接受，云计算也将被各大企业以及独立开发者所选择采用，而对于 IT 从业人员或技术人员来讲，面临的主要影响是自身云技能栈的建立。

云技能栈的建立

目前，各大企业都加大了在云计算上的投入，那么如何将云计算使用好，追求最大的投入回报便成为关键问题。云计算和传统 IDC 有着诸多区别，如果仅仅将云计算当做传统 IDC 来进行使用便达不到上云的目的。简化来看，企业上云的期望主要在于成本优化和效率提升，而技术人员需要通过技能来帮助企业达到这样的目标，势必会对技术人员的技能栈提出新的挑战和要求。

在开始讨论云技能栈的挑战前，先回顾下云计算的三类服务：IaaS（基础设施即服务）、PaaS（平台即服务）以及 SaaS（软件即服务）。

上图展示了不同类型的云计算服务，云厂商和客户的责任分配是怎样的，我们可以根据自身业务的情况来进行灵活的选用，例如类似 GitHub 的 SaaS 类代码托管服务、消息队列 Kafka 这样的 PaaS 类服务以及云服务器这样的 IaaS 类服务，在此我将不再累述了。接下

来主要讲一下云计算给技术人员带来的技能栈方面的挑战，主要在两个方面，分别是对云计算弹性能力的掌握和对云网络与安全架构能力的掌握。

云计算弹性能力的掌握

上云之所以能够有效帮助企业进行成本优化和效率提升，主要是依赖云计算的弹性能力，弹性能力包括资源的快速分配以及资源类型多样性等诸多方面。企业在迁移上云时可能会遇到一些问题，比如业务应用程序架构本身不支持弹性扩展等，这样的情况下将应用迁移上云后，如果业务架构不做出调整，还是无法使用到云计算的弹性能力来帮助优化成本和提升效率。

当然，迁移上云本身会面临新业务应用和遗留业务应用的问题，这里暂不做过多讨论，因此这属于云迁移策略的范畴，还是专注于探讨如何使用好云计算的弹性能力。我将如何使用好云计算弹性能力的要点做了如下简单整理：

1. 业务架构需要采用云优先策略，尽量做云原生（Cloud-Native）架构，使得业务应用本身在基础架构上是对云计算弹性能力有良好支持的，同时，拥抱微服务架构设计风格，使用容器服务来简化运行环境依赖等。
2. 云计算弹性能力的熟悉，例如弹性伸缩（Auto Scaling）、批量计算（Batch Compute）以及无服务函数计算（Serverless Cloud Function）等，简单来说，就是将计算资源的生命周期管理交由云厂商来进行处理，使用者更加关注于业务实现。当然，使用者也可以基于云监控和 API 自行进行资源的弹性扩缩容。不论是何种使用方式，弹性能力是云计算帮助企业优化 IT 成本的基础，能最大程度做到按需使用，减少资源浪费。这里还有个需要注意的地方是关于资源的计算，例如云服务器计费模型的选择问题，不同的计费模式适用于不同业务场景。如间歇、周期性计算作业就适合按量计费这种后付费模式，如长期稳定计算作业就适合包年包月这种预付费模式。
3. 熟悉公有云物理地域和可用区来进行高可用架构设计，充分利用公有云物理地域间内部网络互通的能力。

那么技术人员如何用好云计算的弹性能力呢？目前，主流的云服务商都提供了相关的产品使用介绍资料，如文档、视频以及 workshop 等，通过这些资料可以帮助技术人员快速的熟悉了解云计算的弹性能力。当然，了解熟悉完云服务商提供的弹性计算能力后，我们还需要对自身业务进行梳理分类，来规划好不同业务模块到底应该使用怎样的计算能力。

云网络与安全架构能力

在传统 IDC 模式下，IT 环境更像基于边界的城堡模式，即整座城堡都是由客户自行建立和管理的，而云计算环境更像是一座现代化的酒店，客户在这座酒店可以通过房卡进入特定的楼层和房间。因此不难看出这两种模式下的安全模型是不一样的，如果企业直接将传统 IDC 模式下的安全模型平行迁移到云上，可能会对安全产生不利影响。简单来说，云网络与传统网络模型有相似和不一样的地方，对应技术人员需要掌握的网络相关能力如下：

1. 先掌握私有网络 （Virtual Private Cloud）下的产品，例如子网划分、ACL 设置以及 NAT 网关等产品，最终掌握基于云网络产品的网络隔离方案设计。
2. 了解公网网络计费模型并根据业务特点选用最为适合的计费模型，公有云的公网网络计费有多种模型，适应不同的业务场景，如果不能熟练掌握会造成成本的浪费。例如，公网计费常见的计费模式有按带宽计费、按流量计费等，如果业务类型每日只有很短时间的流量高峰，采用按带宽计费就会有成本的浪费，一般实践而言，当带宽利用率高于 10% 时，建议优先选择按带宽计费。
3. 熟悉公有云特有的网络产品来帮助提高业务效率，例如对等链接、云联网等产品能够帮助提升客户多地域部署时的内部互通性。

正如前面所说云计算更像现代化的酒店，那么云安全架构设计能力就对技术人员提出了如下的基础技能要求：

1. 熟悉云安全责任共担模型，简化而言，就是客户负责使用云的内部安全、云厂商负责云服务本身的安全。使用云的内部安全包括但不限于：数据、身份和访问管理以及操作系统安全配置等。
2. 做好云安全架构指引来帮助企业做好云端安全加固，即云安全架构的能力和产品全景图，以及适合企业业务需要的能力和产品选取方案。

关于云安全架构指引，这里我将分门别类简单整理如下：

1. 基础设施安全：基于私有网络 VPC 设计网络隔离方案、应用防火墙 WAF、安全组（云服务器的网络访问控制）、安全的链路连接（如 VPN 和专线等）等；
2. 身份与访问控制：访问管理系统、多因子认证等；
3. DDoS 防护：云解析（防 DDoS 域名解析服务）、DDoS 防护、安全 CDN、高防 IP 等；
4. 数据加密：块存储及对象存储加密、密钥管理系统、数据库中间件安全连接等；
5. 日志与监控：网络流日志、云审计服务、日志服务、云监控等。

总的来说，做好云安全架构设计，首先需要明确的是文章之前提到的责任模型，即明确哪些责任是由云服务商负责，哪些是由企业自己负责；然后根据上面提到的指引，熟悉并整理出这些产品或功能对企业自身业务的适配程度与边界，如能解决什么问题、不能解决什么问题、解决问题是否引入额外的代价等。这样就明确了手上有哪些弹药，在设计云安全架构时就可以像搭积木一样来进行组合使用了。整体而言云安全架构设计能力是构建于基础的安全架构设计能力之上的，因此掌握基础架构设计知识是前提条件。

从全文不难看出，云计算的普及会对技术人员的使用习惯产生很大的挑战，基础设施工作模式的不一样会带来工作思路的不一样。再加上目前正处于传统 IDC 和云计算并行的阶段，因此对技术人员来说，掌握和了解相关的知识和信息，养成良好的工作习惯是尤为关键的。云计算更多的是服务模式的变化带来了适配工作的挑战，作为技术人员，学会有条理的梳理工作、对数据安全敏感、持续学习等良好的工作习惯，相信面对云计算带来的挑战也将游刃有余。

作者介绍

刘俊强（微信公众号：程序员精进）腾讯云资深架构师、TGO 鲲鹏会会员，曾任迅雷技术总监、某互联网公司技术副总裁，10+ 年以上互联网开发经验，8 年以上技术管理经验。

上一篇　第193讲 | 崔俊涛：如何做好技术团队的激励（下）

下一篇　第195讲 | 吴晖：企业B2B服务打磨的秘诀—ESI

精选留言

写留言

> 由作者筛选后的优质留言将会公开显示，欢迎踊跃留言。