# 云原生的前世今生

随着公有云和私有云的广泛部署，云计算基础设施成为了企业部署新业务的首选。可以说，云计算已进入下半场，各大云计算服务商的厮杀日益激烈，新的概念也层出不穷。近年来，云原生计算（Cloud Native Computing）越来越多地出现在人们的视野中，那么云原生计算与传统云计算相比有什么不同，能利用云原生计算解决什么问题，本章我们将介绍云原生计算的概念和应用场景，并且给出云原生计算的框架。

## 前云计算时代

自计算机发明后到很长一段时间内，计算的目标始终是求解非常复杂的数学问题，如 1946 年第一台计算机埃尼阿克（ENIAC）目的是计算弹道，1999 年著名的网格计算项目 SETI@home1为了寻找外星人的踪迹。那么为了在有限时间内完成计算目标，就需要设计集群化的体系结构，构建强大的计算能力。

在传统计算模式中，通常通过聚集多计算资源进行计算任务拆分、任务调度和计算结果汇聚。

例如，并行计算（parallel computing）通常是在专门设计的、含有多个处理器的超级计算机，通过并行计算机网络将处理机或处理器相连。在物理层面，并行网络中的延迟很低，软件层面，MPI 通信协议和相应软件库可完成不同任务的协同，所以并行计算机可表现出强大的计算性能。如无锡的“神威·太湖之光” 安装了 40960 个中国自主研发的“申威 26010”众核处理器，峰值速度为 125,436 TFlop/s，在 2019 年 11 月最新的榜单中名列世界第三[2]。

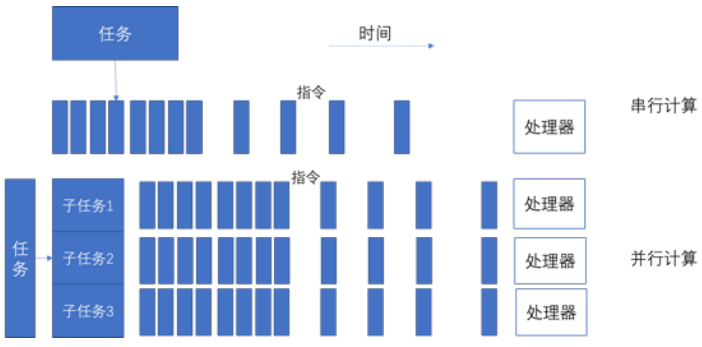


图 0.1 串行计算与并行计算示意图

[1] https://setiathome.berkeley.edu/
[2] https://www.163.com/dy/article/F547LMA005168K55.html

在更通用的场景中，通过计算机网络和普通的计算节点可以形成分布式的超级计算机。交换机、路由器等网络设备彼此相连，通过 TCP/IP 协议组成计算机网络；每个计算节点（如服务器、台式机、笔记本等）有完整的硬件、引导程序、操作系统、中间件和软件栈，并通过网络接口接入计算机网络；借助并行分布式计算技术、网格计算，将计算节点进行统一的任务调度，最终完成复杂的计算任务。

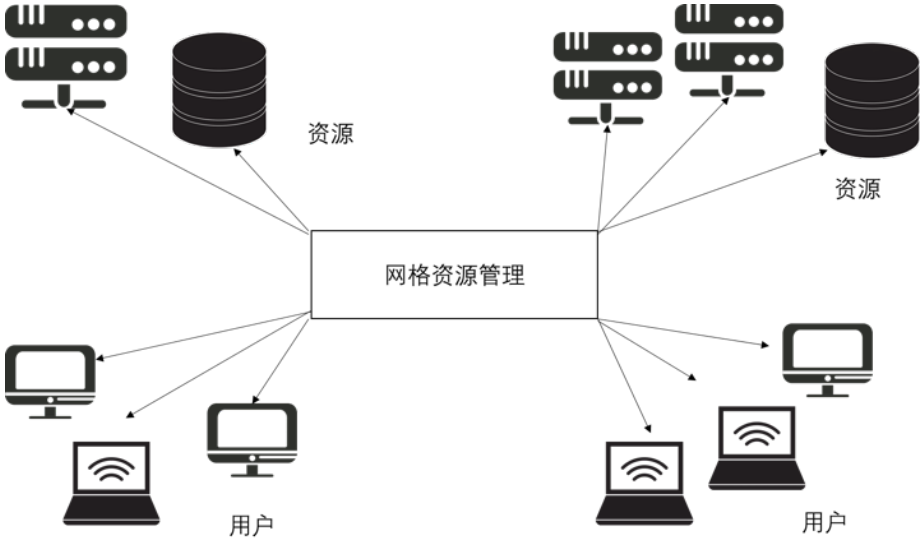


图 0.2 网格计算

如最经典的网格计算项目 SETI@home（Search for Extraterrestrial Intelligence at home）计划，是美国加州伯克利大学于 1999 年正式启动，目的是将从射电望远镜收集到的海量数据中搜寻外星文明信号的任务，外包给全球的普通计算机。BOINC（Berkeley Open Infrastructure Network Computing）[3] 是支撑 SETI@home 的网格计算分布式中间件，当前已经拥有 720,361 台计算机，算力为 27,369 TFlop。相关研究影响了二十一世纪前十年的网格计算发展路线，不过 2020 年 3 月 SETI@home 项目不再分发任务，进入休眠状态，意味着一个时代的谢幕。

[3] https://boinc.berkeley.edu/

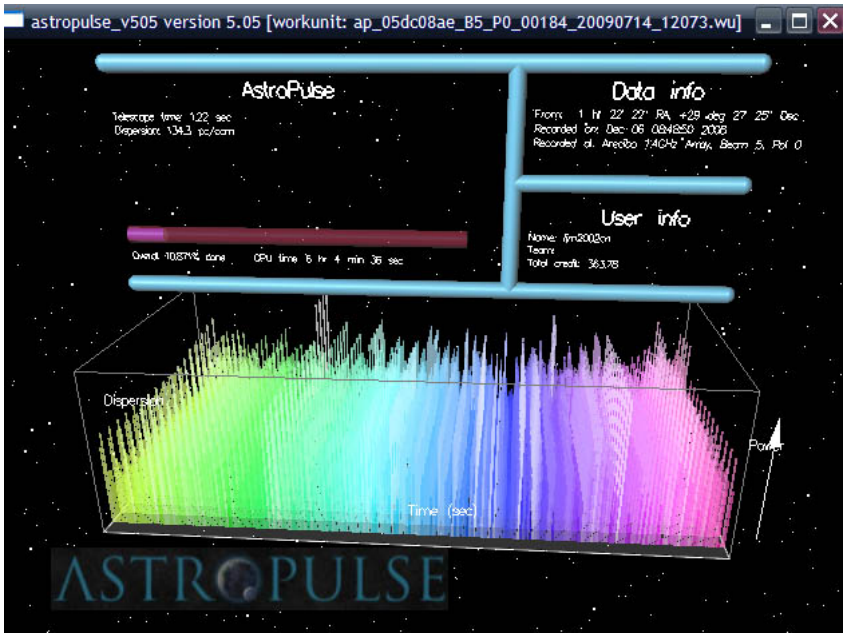


图 0.3 AstroPulse 界面

## 云计算上半场

2006 年，电子商务服务商 Amazon 上线了云计算服务 AWS，包括计算服务 EC2、存储服务 S3 和队列服务 SQS。Amazon 对外提供计算、存储资源的租用，以 AWS 的营收弥补在销售淡季服务器所需的各项成本。经过十多年的发展，云计算已经成为如水电气一样人们习以为常的计算资源和计算模式。从云计算市场看，全球 IaaS 云服务商 2020 年营收为 491 亿美元，同期 SaaS 云服务商营收为 948 亿美元，云安全服务营收为 122 亿美元，云服务相关营收总计 2143 亿美元，增长率为 17.5%。可见其市场广阔，增长率仍很高[i]。

有意思的是，网格计算的网格（Grid）的概念就是源于电网4，其本意是提供一种如电力一样即插即用的普适资源。然而，网格计算主要还是面向科学计算领域，没有经过商业化运作，所以也就没法通过商业变革创造一种新的计算模式。而亚马逊 CEO 杰弗里·贝索斯在推出 AWS 时，就坚信要提供一种普适的基础设施服务。从自身角度看，云计算的确具备了如秒级启动、弹性扩容、随时访问等 “Grid” 所具备的特点。

读者需要注意的是，虽然如很多其它新技术一样，云计算起源于美国，但千万不要照搬美国的云计算发展过程到国内复制一套相似的产品。事实上，中

4 如国家电网叫做 State Grid

国的云计算和云安全发展表现出了鲜明的“中国特色”，这与国内的国情是有密切关系的。

具体而言，美国的云计算发展是先 SaaS 后 IaaS 的阶段。

虽然云计算传入中国最早的印象是 Amazon 的 EC2，但事实上 SaaS 是最早的云计算服务形态。如早在 1999 年，前 Oracle 执行官 Marc Benioff 就创办了 Salesforce，也是当前最大的 CRM SaaS 服务提供商，此外，如在线存储服务 Box 是成立于 2005 年，经过二十年的发展，美国的 SaaS 服务已经深入企业业务，平均每个企业会用到 1427 个云服务，每名员工平均会用到 36 个云服务 5。SaaS 的安全防护主要是以云安全访问代理（Cloud Access Security Broker，CASB）为主，即通过应用层代理的方式部署，并对应用进行检测和防护。因为 SaaS 的广泛应用，所以国外的 CASB 市场巨大，其挑战主要在于需要适配大量 SaaS 服务，所以这个市场的玩家目前主要是如 Skyhigh、Netskope 等巨头为主。

而近几年来，随着企业进一步云化业务，特别是将存量的 IT 基础设施替换为公有云 IaaS 服务中的虚拟计算资源，以提高业务弹性和降低成本，通过软件定义广域网 SDWAN 连接分支结构、云端资源，形成全栈云化，全分支机构云化的趋势。此时，虽然 IaaS 整体营收还远不及 SaaS，但其增长率激增，2019 年的公有 IaaS 服务增长率达到了 37.3%[ii]，远超云服务总体增长率（17.5%）。如 AWS 这样的公有 IaaS，其安全防护主要是利用 Amazon 提供的各类接口，在虚拟网络、虚拟机层面提供网络和终端防护，Gartner 把虚拟机层面的安全防护技术称为云工作载荷防护平台（Cloud Workload Protection Platform, CWPP）。

然而，中国的云计算发展则是从虚拟化起步，从私有云到公有、行业云，走出了具有中国特色的发展路线。

最早在 2000 年以后，VMWare 进入中国时，引入了商业级的虚拟化解决方案，国内企业开始接触到虚拟化技术，当然这远远谈不上云计算，甚至连私有云都不算。

具有里程碑的标志是开源的 IaaS 项目 Openstack 在国内兴起，Openstack 是由公有云服务商 Rackspace 和 NASA 发起，最初是对标 Amazon EC2，目标是构建组件化的、开源的公有 IaaS 平台并提供服务。随着国内云计算需求的不断增强，国内厂商，如华为、华三、EasyStack 等企业基于 Openstack 研发了各

5 数据来自 Gartner Security & Risk Management 2019 峰会

自的云平台，此时国内的云计算需求主要是将硬件服务器虚拟化，再加入多租户管理、网络隔离等需求，因而，多数云计算服务商提供的是私有云的解决方案，当然这也比纯虚拟化已经进了一大步。通常商用私有云系统是封闭的，缺乏对网络流量按需控制的应用接口，因而，针对这类私有云的安全机制多为安全资源池，即构建独立的安全资源，然后通过路由、VLAN 或开放网络接口将流量牵引到资源池处理。

而随着节约成本、集约化管理和提供增值服务等需求的进一步增强，具有云平台开发能力的服务商基于前述的私有云平台，提供了公有 IaaS 的服务。然而，这种公有 IaaS 服务与 AWS EC2、阿里云不太一样，它们具有鲜明的行业特性。例如，为政府提供的政务云，会将所有下属政府机构的服务器迁移到新的云平台上，提供政务相关的服务；而一些大型银行，会为中小银行（包括城商行）提供金融业务相关的 IaaS 和 SaaS 服务，由于金融行业的合规性要求相似，这样具有行业属性的云服务能有效降低中小银行上云的成本和合规性风险；在运营商行业，运营商会引导传统的数据中心 IDC 用户，将其服务器迁移到自己的公有云平台上，提供增值服务，进而获得额外的收益。这样的公有 IaaS 服务，本质上是在前述的 Openstack 体系之上封装了自服务功能，提供行业相关的合规服务和增值服务，因而其安全防护技术也可以基于安全资源池之上，提供面向租户的安全即服务（Security as a Service）。

预计随着新基建的大力推进，公有 IaaS 的市场仍会快速增长，相关的安全投入也会有持续增加。

云计算安全的投入增加，不仅仅是云计算增长对其自身安全业务影响的伴生效应，还在于客户已经对云安全服务这种模式的认可。虽然 2019 年云服务营收的增长率为 17.5%，而 Gartner 预测在 5 年内，云安全订阅服务在总的安全投资比重中会增长 37%[iii]，可见客户对云安全的重视程度。

云计算安全始终是制约云计算被广泛接受的重要因素，纵观云计算发展至今，云计算用户群中始终存在两种矛盾的观点：

**观点 1：“多租户比传统计算更不安全”这个顾虑还是很强且持续**

**观点 2：公有云计算安全的信心在增长**

一方面，云计算中最根本的安全问题为云计算服务商是否可信，云计算用户将数据控制权交给了云服务商，以换取弹性敏捷、冗余灾备等优良特性，那么，保存在云平台上的数据是否会被互联网上的攻击者或云服务商内部的恶意

员工窃取，则是上云的企业至今为止无法消除的疑惑和顾虑。此外，数据可控的合规性压力始终存在，如国外 PCI/DSS、GDPR、CCPA，以及国内的等级保护 2.0 等，对云服务提供商、云计算用户等角色都提出了要求。

另一方面，从统计数据来看，云计算市场的增速相当高。IDC 发布的《中国公有云服务市场（2019 上半年）跟踪》报告显示，2019 上半年中国公有云服务整体市场规模（IaaS/PaaS/SaaS）达到 54.2 亿美元，其中 IaaS 市场增速稳健，同比增长 72.2%，PaaS 市场增速有所回落，同比增长 92.6%。

可见，云计算作为一种革命性的技术体系、运营模式、商业模式，已经成功被大部分企业所接受。知名咨询公司 Gartner 在 2017 年做出如下数个预测[iv]：

**预测 1:在 2020 年前，50%的企业将业务工作流放到本地需要作为异常事件进行审批。公司“无云”的策略会和现在“无网络”的策略一样少**

**预测 2: 在 2019 年前，超过 30%的 100 家最大厂商的新软件投资会从“云优先”转到“只有云”**

**预测 3:在 2022 年前，我们不会认为“云计算”是异常的场景，反而会使用“本地计算”这词去描述不常见的场景**

可见，云计算应用在 2020 年已经成熟，企业上云已经成为一种默认选项。除了渐进式的产业升级、人们观念改变等因素外，近两年的一些趋势发展，使得云计算接受程度增加、云业务变革到来，具体有以下几点：

1. 行业云、政务云兴起，将大量具有类似需求的用户的基础设施、平台和应用部署在一个云计算系统上，可以提升整体运营能力，降低边际成本，在典型领域，如政府、金融、运营商，近年新建的集约化云平台，使得大量传统 IT 系统云化。
2. 5G、边缘计算等新基建热潮。5G、边缘计算和工业互联网的业务场景虽然与传统云计算有较大差异，但这些系统的基础设施均基于虚拟化、容器等技术，所以可以认为是云计算在垂直领域中的应用。新基建的大量投入，也会扩大整个云计算市场的容量。
3. SDWAN。软件定义广域网以较低成本实现了分支机构多地互联的问题，特别是 5G 的切片技术能实现按需的服务质量，会进一步弱化以往

昂贵的专线。那么大量的服务会下沉到 SDWAN 网络中，形成云化资源。

4. 新冠疫情。谁也没有想到的是，2020 年上半年的新冠疫情全球蔓延，大量企业员工在家办公，现场商务会议取消。结果是企业接受远程办公、远程会议等工作、沟通模式，亟需各类支撑业务的 SaaS 服务，很有可能疫情会变成促使国内外 SaaS 增长的重要动力。

综合而言，云服务商提供了成熟的虚拟化基础设施，企业客户也做好了上云的思想、技术和体系的准备，整个云计算的势头已起。

如果说 2020 年云计算的玩家已经踢完了上半场：那么云计算的下半场在哪里，会出现哪些玩家，云服务商、企业客户又将会做什么准备呢。

## 云原生：云计算下半场

近年来，云计算的模式逐渐被业界认可和接受。在国内，包括政府、金融、运营商、能源等众多行业，以及中小企业，均将其托管业务的基础设施进行不同程度的云化。但大多数利用开源或商业的 IaaS 系统构建云计算平台，简单地将传统物理主机、平台或应用转为虚拟化形态。这种方式所带来的好处是整体资源利用更加合理，集约式的运营降低成本，提升整体水平。但总体而言，这样的上云实践只是“形”上的改变，还远没有到“神”上的变化。

云计算的下半场，应该是充分利用云计算弹性、敏捷、资源池和服务化等特性，解决业务在开发、运行整个生命周期中遇到的问题。毕竟，业务中出现的问题，才是真正的问题。

比如，传统应用有升级缓慢、架构臃肿、无法快速迭代等问题，于是云原生（Cloud Native）的概念应运而生。所以，笔者认为云原生就是云计算的下半场。谁赢得云原生的赛道，谁才真正赢得了云计算。

谈到云原生，不能不提始终推动云原生发展的云原生计算基金会（Cloud Native Computing Foundation，CNCF）。CNCF 是一个孵化、运营云原生生态的中立组织，截止到 2020 年 CNCF 共有 371 个开源项目，1402 个项目和组织[4]，可以说是一个覆盖面相当广的云计算组织。国内有 155 个项目和组织积极参与云原生生态圈，共贡献了 21 个开源项目，其中著名的容器仓库 Harbor 就是出自 VMWare 中国团队。

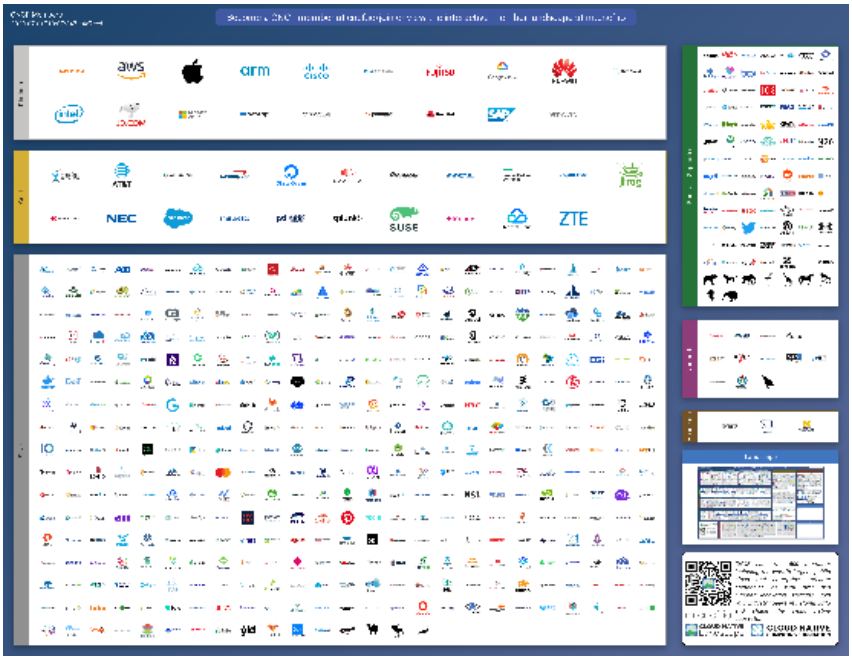


图 0.4 CNCF 全景图

CNCF 对云原生的见解[v]是 “云原生技术有利于各组织在公有云、私有云和混合云等新型动态环境中，构建和运行可弹性扩展的应用。云原生的代表技术包括容器、服务网格、微服务、不可变基础设施和声明式 API。这些技术能够构建容错性好、易于管理和便于观察的松耦合系统。结合可靠的自动化手段，云原生技术使工程师能够轻松地对系统作出频繁和可预测的重大变更。”

云原生提倡应用的敏捷、可靠、高弹性、易扩展以及持续的更新。在云原生应用和服务平台构建过程中，近年兴起的容器技术凭借其弹性敏捷的特性和活跃强大的社区支持，成为了云原生等应用场景下的重要支撑技术。无服务、服务网格等服务新型部署形态也在改变云端应用的设计、开发和运行，从而重构云上业务模式。

## 云原生特征

与虚拟化为基础的传统云计算系统相比，云原生体系一般有如下特征：

### 轻快不变的基础设施

云原生是面向应用的，而非面向基础设施的。在传统虚拟化环境中，应用部署在虚拟机中，虽然虚拟机的生命周期比物理机短，但通常也是以月为单位的，应用安装、更新都需要在虚拟机中完成，因而相对而言，虚拟机的生命周期是长期，虚拟机上的文件系统、运行时环境是动态变化的。

而在云原生环境中，其支撑基础设施通常是容器技术，容器生命周期极短，大部分是以秒和分钟为单位，其占用资源与虚拟化相比也极小，所以容器的最大特点就是轻和快。此外，正是因为容器有轻和快的特点，在实践中通常不会在容器中安装或更新应用，相反，会更新更为持久化的镜像，通过编排系统下载新镜像并启动相应容器，并将旧的容器删除，这种只更新镜像而不改变容器运行时的模式称为不变的基础设施（immutable infrastructure）。从不变的基础设施就能看出，云原生的运营和传统虚拟机运营方式会是截然不同的。

### 弹性服务编排

云原生的焦点是业务，而非基础设施，而业务的最核心之处的是业务管理和控制，例如服务暴露、负载均衡、应用更新、应用扩容、灰度发布等。服务编排（orchestration）提供了分布式的计算、存储和网络资源管理功能；按需、弹性地控制服务的位置、容量、版本；监控并保证访问的可用性。

服务编排对应用层隐藏了底层基础设施的细节，但又提供了强大的业务支撑能力，以及让业务正常运行的容错、扩容、升级鞲能力，使得开发者可以聚焦业务本身的逻辑。

### 开发运营一体化

开发运营一体化（DevOps）是一组将软件开发和 IT 运营相结合的实践，目标在于缩短软件开发周期，并提供高质量软件的持续交付。虽然 DevOps 不等同于敏捷开发，但它是敏捷开发的有益补充，很多 DevOps 的开发理念（如自动化构建和测试、持续集成和持续交付等）来自于敏捷开发。与敏捷开发不同的是，DevOps 更多地在消除开发和运营侧的隔阂，聚焦在加速软件部署。

当前，很多云原生应用的业务逻辑需要及时调整，功能需要快速丰富完善，云端软件快速迭代，云应用开发后需要快速交付部署，因而开发运营一体化深深地融入到了云原生应用整个生命周期中。

### 微服务架构

传统 Web 应用通常为单体应用系统，如使用 Websphere、Weblogic 或.Net Framework 等，从前端到中间件再到后端，各个组件一般集中式地部署在服务器上。

后来随着 Web Service 的标准（UDDI、WSDL、SOAP）推出，应用以标准的服务交付，应用间通过远程服务调用进行交互，形成了面向服务的架构（Service-Oriented Architecture，SOA）。SOA 极大提升了应用组件的标准化程度和系统集成效率。

在云原生应用设计中，应用体量更小，因而传统单体应用的功能被拆解成大量独立、细粒度的服务。微服务的架构，使得每个服务聚焦在自己的功能，做到小而精，然后通过应用编排组装，进而实现等价于传统单体应用的复杂功能。其优点是后续业务修改时，可复用现有的微服务，而不需要关心其内部实现，最大程度减少重构开销。

## 无服务模型

无服务（Serverless）是一种基于代码和计算任务执行的云计算抽象模型，与之相对的是基于服务器（虚拟机、容器）的计算模式。无服务在公有云和私有云都有相应的服务，例如 AWS Lamda、阿里云的函数计算，Kubernetes 的 Kubeless、Apache OpenWhisk 等。无服务的模式改变了以往人们对计算的认知：

1. 传统的计算通常是由将任务分发到某个节点，然后通过任务/进程/线程启动计算，结束后返回。而无服务不使用长期独占的进程，而是使用了事件驱动的函数计算，将计算任务分散到极细颗粒度的各种函数，因而计算任务可以被分布式部署，每个任务都是轻量级的，容易调整计算逻辑。
2. 由于不需要考虑具体的资源部署机制，所以能够极大简化计算任务部署流程，加速业务上线和更新的速度，也节省了管理计算资源的运营成本（OPEX）。
3. 无服务提供了最小暴露面和最短执行时间，所以可以有效的缓解针对业务的威胁。

总体而言，云原生真正地以云的模式管理和部署资源，用户看到的将不是一个个 IT 系统/虚拟主机，而是一个个业务单元，开发者只需要聚焦在业务本身，可以说微服务的设计、无服务的功能正是云原生理念的核心体现，而容器、编排、服务网格均是实现云原生的支撑技术。理解这一点，才有可能真正做好云原生安全。

## 小结

云原生是云计算时代的下半场，或许我们可以称之为云计算 2.0。云原生的出现，与云计算不断与具体业务场景融合，与开发运营一体化碰撞的结果，是一场由业务驱动的对云端基础设施、编排体系的重构。

云原生系统与业务系统运营有很强的关系，又要支撑不断演进的快速开发、快速交付模式，可预见云原生安全除了基础设施安全、IT 运营安全外，将会覆盖应用安全、业务安全、开发安全等内容，而且这些细分的安全功能，应该是通过有机、一致的形式共同作用于云原生环境。

---

[i] Gartner, Gartner Forecasts Worldwide Public Cloud Revenue to Grow 17.5 Percent in 2019, https://www.gartner.com/en/newsroom/press-releases/2019-04-02-gartner-forecasts-worldwide-public-cloud-revenue-to-g

[ii] Gartner, Gartner: IaaS Public Cloud Services Market Grew 37.3% In 2019, https://www.crn.com/news/cloud/gartner-iaas-public-cloud-services-market-grew-37-3-in-2019

[iii] Gartner, The State of Network Security in the Cloud Era, Gartner Security&Risk Management Summit, MD, 2019

[iv] Gartner, Gartner Says By 2020, a Corporate "No-Cloud" Policy Will Be as Rare as a "No-Internet" Policy Is Today, https://www.gartner.com/en/newsroom/press-releases/2016-06-22-gartner-says-by-2020-a-corporate-no-cloud-policy-will-be-as-rare-as-a-no-internet-policy-is-today

[v] CNCF Cloud Native Definition v1.0 ，https://github.com/cncf/toc/blob/main/DEFINITION.md#中文版本