简译版

云中进行网络监控的三种方法

非官方中文译文·安天技术公益翻译组 译注

文档信息			
原文名称	Network Monitoring in the Cloud: 3 Options		
原文作者	Andrew Froehlich	原文发布日期	2018 年 7 月 23 日
作者简介	Andrew Froehlich 是 West Gate Networks 公司的总裁。 https://www.networkcomputing.com/author/16268793		
原文发布单位	Network Computing		
原文出处	https://www.networkcomputing.com/networking/network-monitoring-cloud-3-options/1040257935		
译者	安天技术公益翻译组	校对者	安天技术公益翻译组
分享地址	请浏览创意安天论坛 bbs.antiy.cn 安天公益翻译板块		
免责声明	• 本译文译者为安天实验室工程师，本文系出自个人兴趣在业余时间所译，本文原文来自互联网的公共方式，译者力图忠于所获得之电子版本进行翻译，但受翻译水平和技术水平所限，不能完全保证译文完全与原文含义一致，同时对所获得原文是否存在臆造、或者是否与其原始版本一致未进行可靠性验证和评价。 • 本译文对应原文所有观点亦不受本译文中任何打字、排版、印刷或翻译错误的影响。译者与安天实验室不对译文及原文中包含或引用的信息的真实性、准确性、可靠性、或完整性提供任何明示或暗示的保证。译者与安天实验室亦对原文和译文的任何内容不承担任何责任。翻译本文的行为不代表译者和安天实验室对原文立场持有任何立场和态度。 • 译者与安天实验室均与原作者与原始发布者没有联系，亦未获得相关的版权授权，鉴于译者及安天实验室出于学习参考之目的翻译本文，而无出版、发售译文等任何商业利益意图，因此亦不对任何可能因此导致的版权问题承担责任。 • 本文为安天内部参考文献，主要用于安天实验室内部进行外语和技术学习使用，亦向中国大陆境内的网络安全领域的研究人士进行有限分享。望尊重译者的劳动和意愿，不得以任何方式修改本译文。译者和安天实验室并未授权任何人士和第三方二次分享本译文，因此第三方对本译文的全部或者部分所做的分享、传播、报道、张贴行为，及所带来的后果与译者和安天实验室无关。本译文亦不得用于任何商业目的，基于上述问题产生的法律责任，译者与安天实验室一律不予承担。		

云中进行网络监控的三种方法

Andrew Froehlich

2 018 年 7 月 23 日

当企业连接到公共云服务时，其网络团队可以采用以下三种方法来监控网络性能。

随着企业进一步扩展到公共云，其构架师面临着这样一个问题：应该如何监控网络设备以及采用不同构架的云如何互联？答案可能多种多样，它取决于企业采用的具体的云构架方式。在某些情况下，可以使用云服务提供商（CSP）提供的内置监控/告警工具。在另一些情况下，传统的监控工具效果可能会更好。如果既想要更好的可视性，又想要卓越的告警能力，那么还可以使用以云为中心的网络性能监控工具。在本文中，我们将看看以上介绍的三种不同工具在不同的用户场景下的选择策略，以及各自的优缺点。

CSP 提供的网络监控工具

到目前为止，在云中进行网络监控最便宜、最快捷的方法是使用 CSP 提供的工具。例如，AWS 允许客户使用 CloudWatch 来监控亚马逊弹性计算云（EC2）实例的入站和出站流量。此外，AWS 允许访问虚拟私有云（VPC）中的客户流数据。启用并配置 CloudWatch 后，管理员可以根据各种日志和流触发器来创建基本告警。

该方法的主要缺点是，CSP 提供的工具只能在单个云中运行。因此，如果你在混合云或多云环境中运行，你将需要管理多个监控/告警平台。你还会丧失端到端的可视性，这可能会妨碍云之间特定网络问题的识别和故障排除。那些谨慎对待网络监控的 IT 部门通常仅在监控 DevOps 环境，或者云提供商的应用程序和数据对企业业务影响较小时，才会使用此类工具，原因就在于此。

传统的网络监控工具

在可行的情况下，大多数企业会在公共云网络中部署传统的网络监控工具，如 ping，SNMP 轮询和 NetFlow。这样做的好处是，网络管理员用于监控企业 LAN 和 WAN 组件的工具，也可以用于监控云实例。

云计算

该方法的主要缺点是，在云环境中部署传统网络监控工具并不总是可行的。对于“基础设施即服务”（IaaS）云来说，这种部署很容易实现；但对于“平台即服务”（PaaS）和“软件即服务”（SaaS）云来说，许多传统的网络管理工具都无法运行。因此，你可能只能使用 ping 和 traceroute 等非常基本的监控工具，而无法使用 SNMP 轮询和 Netflow 等更强大的工具。

该方法的理想用户场景是混合云架构——私有云连接到公共 IaaS 云。在这种情况下，管理员可以简单地将已经部署的企业 LAN 网络监控工具扩展到 IaaS 实例，以实现端到端的可视性。该方法的优点是部署和管理很容易，而且成本很低。

以云为中心的网络性能监控工具

相比于企业 LAN 能够提供的网络可视性，很多 IT 部门的要求会更高一些。由于企业已经将一定权限（信任）赋予 CSP，因此 IT 团队需要增加可视性，以便更密切地关注云内部和出入云的网络性能。最近，网络监控市场上出现了各种以云为中心的网络性能监控平台，它们大多来自思科、ExtraHop 和 ThousandEyes 等公司。其中的许多平台包括网络探针、云代理以及深度路由和策略更改通知。这些工具可为最终用户提供细粒度的网络运行状况信息。

这些工具的缺点是成本较高和管理复杂。但是，如果企业运行着对业务有重要影响的应

用程序和数据，并且在复杂的多云架构中运行，其优点往往会碾压这些缺点。

安天简介

安天是引领威胁检测与防御能力发展的网络安全国家队，安天依托下一代威胁检测引擎、主动防御内核等自主先进技术、“赛博超脑”支撑平台和专家团队，为用户提供端点防护、流量监测、快速处置、深度分析等产品，以及安全管理、威胁情报、态势感知和靶场演练等解决方案。

安天为国家主管部门、军队、保密、部委行业等高安全需求部门，提供高级威胁和新兴威胁解决方案和能力体系，产品与服务保障了“载人航天”、“探月工程”、“空间站对接”、“大飞机首飞”等重大国防军工任务。安天也是全球重要的基础安全供应链上的核心节点，全球近百家著名安全厂商、IT 厂商选择安天作为检测能力合作伙伴，安天的检测引擎为全球近十万台网络设备和网络安全设备、超过十亿部智能设备提供安全防护。其中移动检测引擎是全球首个获得 AV-TEST 年度奖项的中国产品。

安天技术实力得到行业管理机构、客户和伙伴的认可，安天已连续五届蝉联国家级安全应急支撑单位资质，亦是中国国家信息安全漏洞库六家首批一级支撑单位之一。安天是中国应急响应体系中重要的企业节点，在红色代码、口令蠕虫、心脏出血、破壳、魔窟等重大安全威胁和病毒疫情方面，提供了先发预警和全面应急支撑。安天针对震网、毒曲、火焰、沙虫、方程式、白象等 APT 组织或 APT 行动，进行了深度的解析，对捍卫国家主权、安全和发展利益形成了有利的支撑。

在 2016 年 4 月 19 日由习近平总书记召开的网络安全和信息化工作座谈会上，安天创始人、首席技术架构师作为网络安全领域的发言代表，向习总书记进行了汇报。2016 年 5 月 25 日，习近平总书记在黑龙江调研期间，视察了位于哈尔滨科技创新城的安天公司，对安天负责人说，“你们也是国家队，虽然你们是民营企业”。

安天实验室更多信息请访问： *http://www.antiy.com（中文）*

http://www.antiy.net（英文）

安天企业安全公司更多信息请访问： *http://www.antiy.cn*

安天移动安全公司（AVL TEAM）更多信息请访问： *http://www.avlsec.com*