



DeepFlow[®]

云网分析

云网络流量采集
可视化与分析

DeepFlow[®] Product White Paper v5.6

DeepFlow[®] 摘要



当业务上云 遭遇监控盲区

云网络的流量巨大
云网络监控点不足
云网络故障排查困难

赋能云网络的 SDN 价值

混合云网络全栈监控架构
DeepFlow[®] 产品三大组件

DeepFlow[®] 产品特性

云网络的知识图谱
统一的抽象采集层
云原生部署和扩展
监控能力随云扩展
高性能的采集技术

DeepFlow[®] 产品适用场景

适用场景一：混合云网络流量采集
适用场景二：混合云网络性能监控
适用场景三：业务网络全链路追踪
适用场景四：混合云全栈网络分析

总结



DeepFlow[®] Executive Summary 摘要

云服务在各行业中的占比越来越大。除了宏观指导政策，自 2017 年起，我国已有 70% 以上的省市先后出台政策，推动当地企业加速上云。但企业上云不同程度地遭遇虚拟网络黑盒的挑战，DeepFlow[®] 是北京云杉世纪网络科技有限公司（以下简称云杉网络）推出的一款云网络流量采集、可视化与分析产品，解决企业上云遇到的业务网络全链路、多维度可观测性难题。DeepFlow[®] 软件支持集群部署，支持容器（Kubernetes）、OpenStack、vSphere 虚拟化环境和 AWS、阿里云、腾讯云等多种云环境，帮助企业在混合云环境中统一采集并分发任意工作负载之间的网络流量，实现对云端业务全链路的性能监控和多维度的可观测性。凭借领先一代的技术优势和完整的产品解决方案，DeepFlow[®] 已在 50 多家世界 500 强企业落地部署，不断为客户提供云网络治理的最佳实践。

When Business Encounters **Monitoring Blind Spots** After Migrating to Cloud

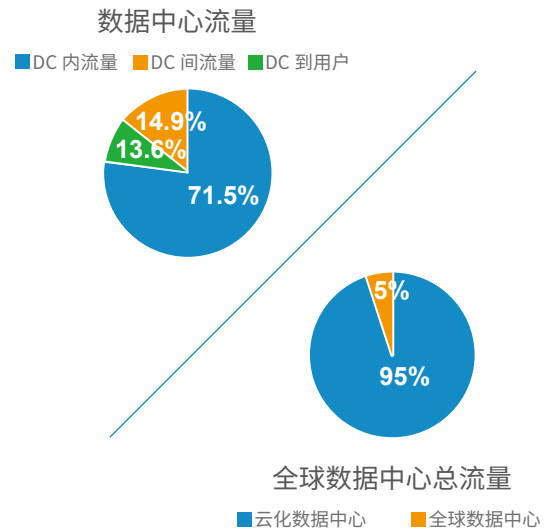
当业务上云
遭遇监控盲区



虚拟网络为云上业务带来了租户隔离、快速部署、灵活扩展等优势。然而，由于传统面向物理网元设备的网络监控无法直接应用于云内的虚拟网络，因此虚拟网络成为了业务上云后的监控盲区。不同于物理网络监控，虚拟网络监控面临全新挑战：

云网络的流量巨大

根据思科的统计数据，2021 年云化数据中心的流量将占全球数据中心总流量的 95% 之多。随着 10G/25G/100G 网卡在数据中心的普及，面对大规模的虚拟网络流量，传统的采集手段显然无法满足快速排障的要求，在云架构下必须依靠带内遥测技术（In-band Telemetry）和实时数据分析手段方能应对超大规模虚拟网络流量的监控需求。对于特定的监控和分析对象，需要充分利用云计算分布式的特性，本地化地完成虚拟流量的预处理，才能满足其要求。



云网络监控点不足

我国金融云的建设和发展相对领先，等保 2.0 国家标准的施行进一步加强对金融业务上云的监管要求。当前中大型金融机构的 IT 基础设施全面池化，使得传统网络的边界延伸到物理服务器内部，而服务器内部的网络层级从虚拟机到容器不断延伸，物理服务器内部不同虚拟网元之间的流量交互不再完全经过物理交换机。由于传统网络监控方案只能满足物理服务器外部的需求，无法强化地甚至无损地移植到云环境中，随着虚拟网络的规模和层级不断增长，再加上虚拟网元频繁变化的特性，使得虚拟网络中的监控盲区越来越大。企业亟需针对虚拟网络部署更多的监控点、并梳理新的指标体系，以满足监管合规要求。



云网络故障排查困难

大规模的企业和组织中，经常出现多种厂商、多种型号设备并存的情形，不同的监控分析工具通过互相协同可以提供整体的网络故障排查能力。在云时代，由于虚拟网络的规模巨大、层级繁多，容器、虚拟机、服务器、交换机、负载均衡、防火墙等网络服务的访问和依赖关系复杂，在云中如何实时识别类型繁多的虚拟网元及其配置信息、进而在虚拟网络动态变化的前提下实时监控业务网络的运行状态，成为保障云端业务稳定运行的前提。这也是满足企业上云安全、稳定运行保障的核心能力。

The SDN Value of Cloud Networking Enablement

赋能云网络的 SDN价值

云杉网络深耕数据中心网络解决方案多年，认识到要解决上述问题必须深刻理解业务和网络的关系，即将网络的拓扑、网络的流量与其承载的业务进行有机的关联。云杉网络DeepFlow® 从虚拟流量的采集、分发、分析三个层面出发，抽象网络流量数据中的类型、从业务的视角层层梳理网元与流量的特性，从而为客户提供真正有价值的解决方案。

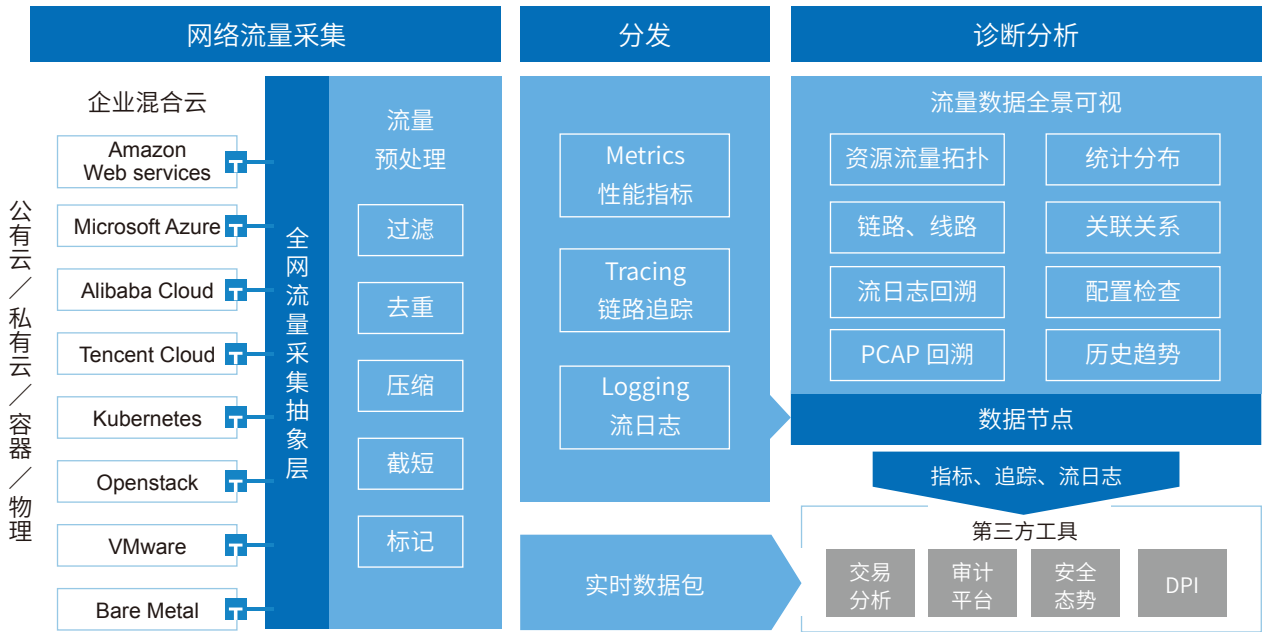
DeepFlow® 重点收集以下三类网络数据

遥测数据：包括指标数据和追踪数据。鉴于网络具备独特的时序性，我们重点收集 Metrics 数据和 Tracing 数据，即资源池内各类网元的实时统计信息，以及网元之间的访问关系。

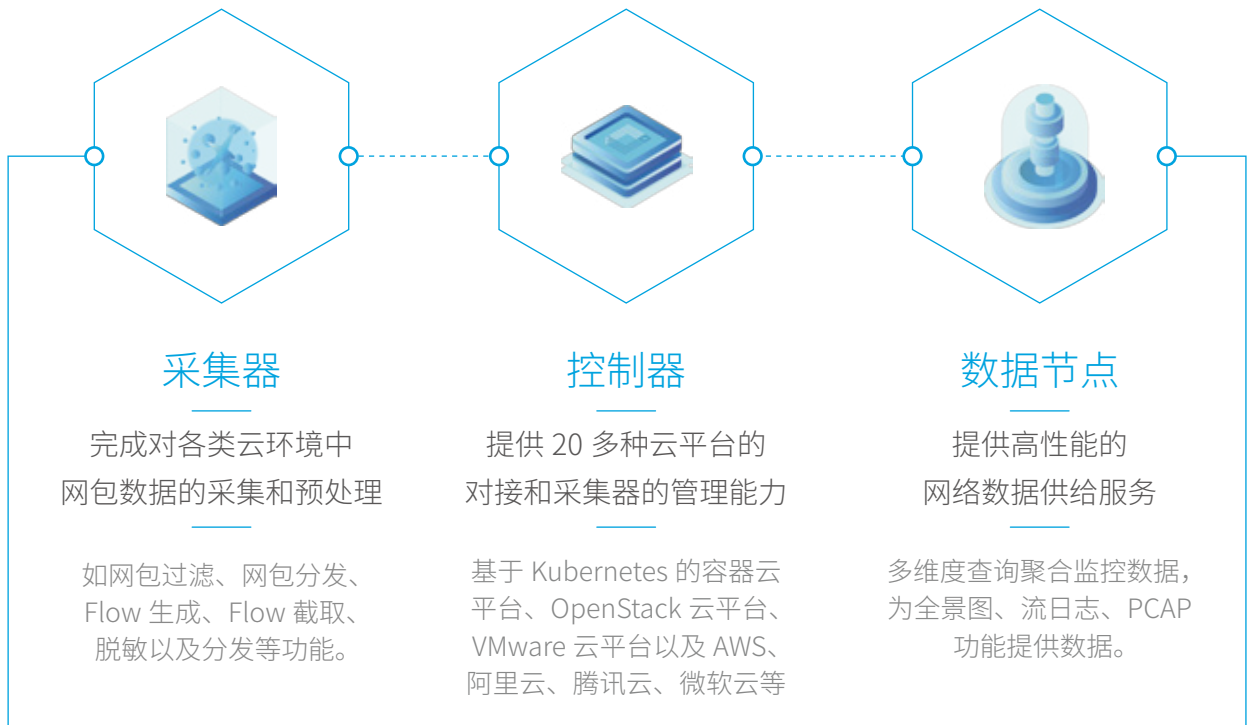
网包数据：即目标业务网络的原始网包，用于分发给后端的分析工具使用，此类数据量与业务流量实际大小相关；网包数据的采集需要在不影响业务的前提下确保精准和高效。

日志数据：即各类流日志、会话日志、应用日志等，用于非实时的回溯查询或数据分析。

混合云网络全栈监控架构



DeepFlow® 产品三大组件





在混合云环境中，业务通常会涉及到不同的资源池、有时甚至经常遇到多数据中心的场景。底层环境包括OpenStack、VMware、裸金属、容器等，从网络区域涉及到业务区、互联网接入区、外联区、DMZ区等，在云计算转型比较深入的企业中，会涉及到更多的网络功能服务链。网络的保障涉及到配置、日志及现网流量或流数据等元素，绘制一张多维度的网络知识图谱是服务监控的基础能力，在DeepFlow全景图中，用户可以透过几十个维度的“网络知识图谱”观察业务实例，并在不同维度和路径之间快速跳转，实现业务网络全景式的可观测性。



为了提升 DeepFlow[®] 的适用性，云杉网络做了大量的工作适配主流的资源平台和云平台，并不是简单调用 API，而是要与知识图谱等对接和关联起来的。目前，DeepFlow[®] 支持与 20 多个市场主流平台做资源信息的同步，通过抽象统一的采集层、构建了较为完备的网络知识图谱的体系。



DeepFlow®采集器拥有不同形态的版本、以进程形态独立运行并支持一键部署,共有包括VMware ESXi采集器、KVM采集器、KVM-DPDK采集器、HyperV采集器、Workload-V/Workload-P采集器、容器OnVM采集器、容器OnHost采集器、专属服务器采集器等多个类型;对于裸金属设备资源池,获取其池内网络流量可通过Leaf交换机、接入交换机的端口镜像,汇总至TAP设备后交由专属服务器类型采集器实现对数据包处理操作,也可以选择将采集器安装在每一台需要采集的裸金属设备系统上。



DeepFlow®控制器按角色分为主控制器、备控制器、从控制器,用户可根据实际部署要求进行灵活选择。单一控制器可管理2000个采集器,足以覆盖一个可用区涉及的采集规模。主、备控制器与从控制器协同工作,控制器集群规模最大支持50台,整体可管理10万台采集器规模,可满足大型企业私有IT、公有云、容器等对云数据中心资源池建设持续演进的网络流量监控分析要求。此外,采集器不再是简单地获取网络流量管道,是具备对本地采集的网络流量进行处理的计算单元,众多采集器以及控制器构建成一个与云网规模一致的分布式流量处理系统。



DeepFlow® 拥有多项专利技术,采集器目前支持 1800 多个监控指标数据(随着版本迭代将持续增加),标准版支持长达 1 年存储、高达 1 秒精度的全栈(网络 + 应用)数据覆盖,满足端到端及服务端口的逐跳流粒度检索能力,全景图实时展示关联至资源池、虚拟化、容器、应用、网络等 30 个资源知识图谱信息。控制器与采集器之间采用加密通信,整体方案可满足 10 万量级采集点的管理。



适用场景一

混合云网络流量采集

DeepFlow® 通过与客户云平台、监控平台的对接，实现虚拟网络流量的按需采集、统一存储、高效分发，解决了混合云环境下网络流量的一体化采集难题。

利用 DeepFlow® 控制器、采集器组件即可实现混合云全网流量采集，通过对接异构资源池管理平台，采集器根据接收到的控制器指令完成混合云资源池流量的全网采集和预处理，并按需地将后端所需的流量通过隧道发送给第三方分发平台或者分析工具。

DeepFlow® 流量采集与分发方案具备较好的平台适应性，支持各类 overlay 网络方案如 Linux Bridge、OVS、VSS、VDS 等，以及基于 underlay 或 overlay 的各类容器网络方案。提供数据包过滤和分发功能，同时能够对数据包进行按需截断以降低监控网络带宽占用。控制器与资源池管理平台对接后能实时感知虚拟机、容器等资源变化，从而使得采集器具备自动跟随能力。整体方案满足 10 万采集点规模的统一管理，过载保护机制确保平台稳定运行且不会对用户云环境造成影响。

价值总结

场景描述

特性介绍



适用场景二 混合云网络性能监控

价值总结

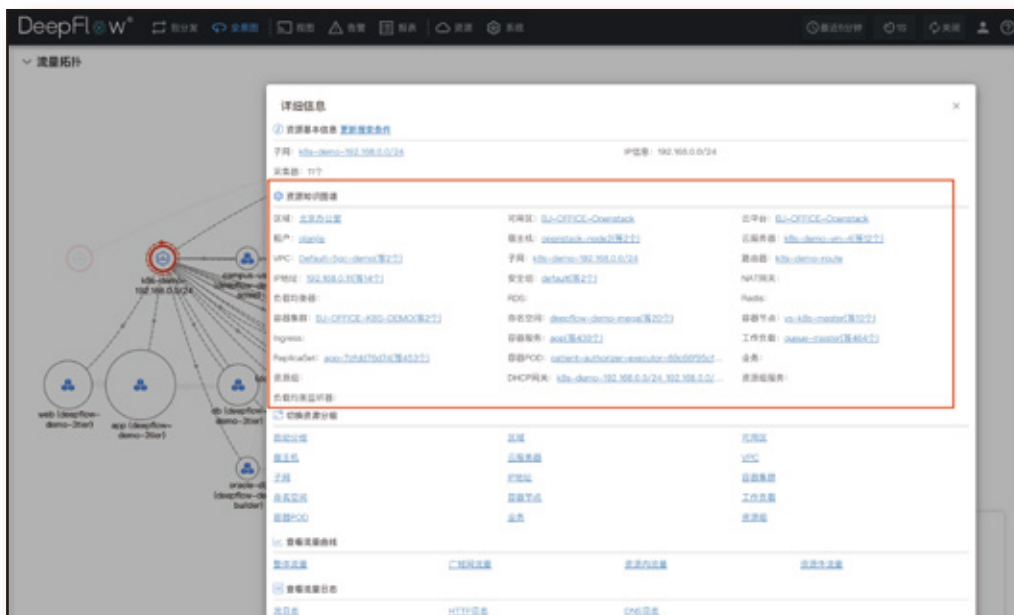
在层次复杂的混合云网络环境中，DeepFlow® 通过构建混合云网络全景图，将网络信息、资源信息、服务信息、及业务信息关联起来，精准呈现链路上不同的节点、路径的流量指标数据如吞吐、负载、时延、性能、异常等性能指标。

场景描述

性能监控利用 DeepFlow® 控制器、采集器和数据节点，对上云的业务网络进行全链路的追踪和监控，实时呈现业务关心的各项网络性能指标，打破了虚拟网络监控的“黑盒”。

特性介绍

DeepFlow® 创新地解决了业务网络的实时监控，无论云中业务如何动态变化，监控策略都能实时自动跟随，基于知识图谱的业务网络全景图满足从全局视角到故障点深度钻取的1800多种性能数据的灵活查看。





使适场景三 业务网络全链路追踪

价值总结

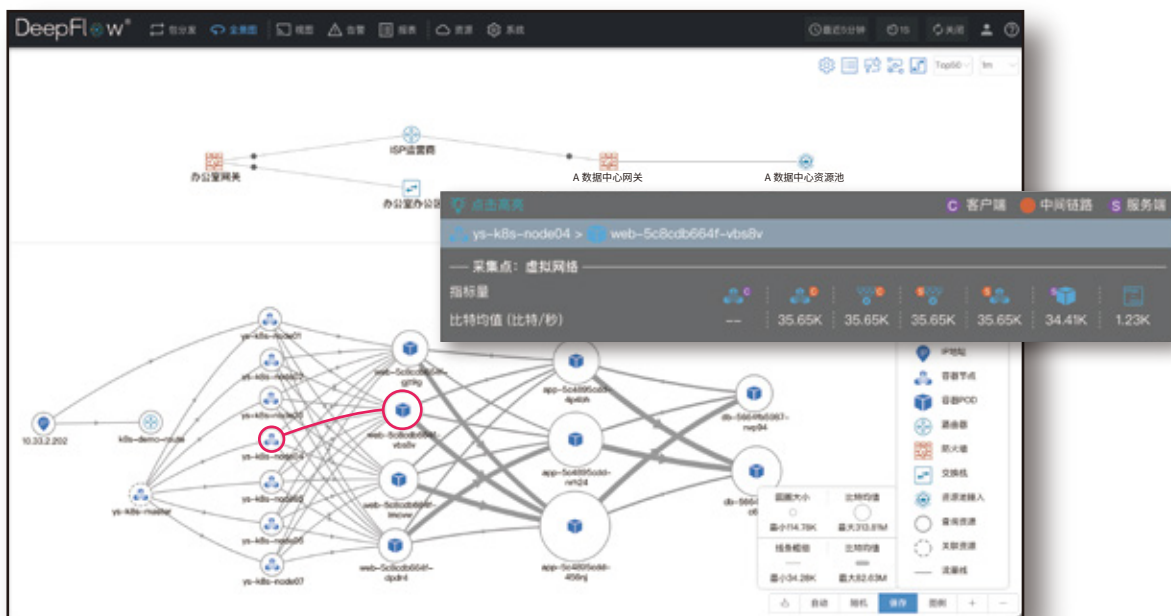
对于云原生业务，用户可通过 DeepFlow[®] 对物理链路、虚拟链路统一进行链路逐跳的排查，快速定位丢包和时延的位置。

场景描述

DeepFlow[®] 通过自动学习资源池里的各类资源信息、采集并分析生产网络中的网元配置和流量信息并绘成知识图谱，用户通过全景图即可方便地进行业务网络端到端的监控分析。DeepFlow[®] 全链路追踪支持从多种维度查看任意网元之间逐段链路的性能指标和流量统计详情，结合告警和报表设置，及时发现潜在风险。

特性介绍

DeepFlow[®] 全链路追踪能够自动检测任意两个网元之间的连通性，用户可排查任意 IP 对、容器 Pod、虚拟网元之间的网络连通质量问题。凭借业务网络全链路的监控能力，确保云端业务的稳定运行。





使用场景四 混合云全栈网络分析

价值总结

对于采用容器混合云部署的业务,借助 DeepFlow® 全栈分析能力用户可从源端物理网络、物理服务器到 OvS、虚拟机、容器的各个层级进行钻取。

场景描述

DeepFlow® 目前实现了全栈覆盖网络 + 应用的流量监控和分析,针对需要钻取或详细查看的环节,用户通过全景图页面从问题地域开始经过物理网络、虚拟网络、虚拟网元等丢包和时延数据的定位,逐级缩小问题范围,并能将故障点与虚拟机、容器 POD 的启停、创建(同步)、删除、迁移、IP 变更事件进行关联展示,还可以跳转到流日志三级页面,查看对应的原始流日志详细信息,或通过精细搜索过滤指定网流的源、目的、协议、服务端口等。

特性介绍

DeepFlow® 已经与市场上主流的 20 多家云平台完成了产品对接,当混合云用户需要对故障点进行钻取分析时,DeepFlow® 的全栈能力让用户排查故障时的体验犹如探囊取物。





目前 DeepFlow® 支持容器 (Kubernetes)、OpenStack、vSphere 虚拟化环境和 AWS、阿里云、腾讯云等各类云环境，帮助企业在混合云环境中统一采集并分发任意工作负载之间的网络流量，实现对云端业务全栈、全链路的性能监控和多维度的可观测性呈现。凭借领先一代的技术优势和完整的产品解决方案，DeepFlow® 已在金融、电信、政务、教育、能源、电力、互联网等行业 50 多家世界 500 强企业落地部署，不断为客户提供云网络治理的最佳实践。

销售热线：400-9696-121
更多信息请访问云杉网络官网
<http://www.yunshan.net>

北京云杉世纪网络科技有限公司
北京市海淀区成府路28号优盛大厦A座1209
市场合作:info@yunshan.net
合作咨询:400-9696-121

版权所有 © 2021Yunshan Networks 保留所有权利。
本资料中的部分插图来自于互联网,文字内容和产品相关图片未经许可禁止擅自摘抄使用。



技术创造价值