DeepFlow® 云网分析

万科多云网络流量管理平台建设实践

1. 万科地产的转型之路

企业对云的认识越来越成熟，行业云、私有云逐渐成为企业的选择。万科企业股份有限公司（以下简称“万科”）对科技、互联网的拥抱由来已久，早年便有向互联网企业学习的历史，王石曾在一次演讲中表示，万科向技术转型是必然的趋势。2016 年万科启动了“沃土计划”，开启了万科内部的一场信息化革命，为保证沃土计划的落地实施，万科组建万翼网络科技有限公司（以下简称“万翼科技”）。

万翼科技是万科集团的全资子公司，是向万科集团以及所有下属子公司、相关关联公司提供 IT 规划、开发和运营服务的 IT 科技服务提供商。万科云正是在这样的背景下迅速发展起来的。随着万科的转型，多元业务战略对业务间整合、客户资源打通、信息系统建设等提出了更高的要求，万翼科技扮演的角色越来越重要。万科希望自己扮演的角色是一个全新的生态构建者、连接者，采用“重服务，偏运营”的方式将产业上下游的要素进行聚集，进而对产业链进行重构，形成新的生态系统。

2. 万翼科技的多云战略

据 RightScale 2019 年云状态报告显示，84%的企业采用了多云战略。混合云的优势在企业上云过程中愈发突显，各大厂商也在混合云市场继续发力使得多云管理、云网协同和安全方面的能力不断提升，混合云在各个行业的应用越来越深入。在这样的背景下，万翼科技选择了多云架构作为集团业务上云的基础支撑。万翼科技在不同阶段分别上线了阿里公有云、微软 Azure 公有云、华为公有云、VMware 私有云、华为私有云共计 5 个云资源池平台以满足业务发展的需要。

2.1. 多云异构带来的挑战

与众多企业一样，虚拟网络如何监控分析成为万科的新课题。万科这 5 朵云由于缺乏有效的虚拟网络分析工具和手段，无法对其进行统一的管理，因此迫切希望构建统一的混合云管理平台提高运营效率，以确保万科云持续高效安全地运行。

业界已形成共识，针对传统网络的监控分析方法无法适应云时代的需求，目前万科云平台在虚拟网络监控分析方面还存在一些空白。采用多云架构之后，万科云的管理团队遇到了基础设施资源池多样化、异构资源池统一监控难、资源和服务的调配能力与效率低等困难。

2.2. 万科 5 朵云的统一流量管理

业界对于多云环境的统一网络监控尚在探索之中。云杉网络 DeepFlow® 独有的采集器技术能够同时运行在不同的资源池环境中，单台控制器可以对接多个不同的云平台和管理数千个采集器，从而实现多云异构环境下统一的网络监控和分析，由此成为市场上能够匹配万翼科技的 5 朵不同云的最佳选择。通过采用 DeepFlow® 方案，万科云得以建设并实现如下目标：

2.2.1. 东西向流量采集能力

针对 5 朵不同的云平台，实现对部分直接在宿主机内部完成传输的东西向流量的采集，破除虚拟网络带来的黑盒效应。

2.2.2. 全网可视化能力

实现包括虚拟网络以及混合网络中端到端的网络可视化，生产网络和业务网络实时数据以及历史网络数据的可视化等。

2.2.3. 基于租户网络的计量能力

通过对接云平台及基于 SDN 的虚拟网络，区分租户网络并实现对租户网络流量精确的采集、统计能力。

2.2.4. 虚拟网络异常感知能力

通过对虚拟网络流量的分析，实现对业务网络变更、网络故障恶化、网络异常的自动感知及告警能力。

3. DeepFlow® 解决方案

万翼科技在经过反复调研和详细沟通后，选择了部署 DeepFlow® 虚拟网络流量采集与分析系统软件，以现有的 5 个云平台网络数据为核心，通过对其虚拟网络流量进行采集和分析，实时监控云平台网络运行情况，保障网络安全高效地运行。

3.1. 方案概述

在万科云项目建设中， DeepFlow® 平台对接范围包括阿里公有云、VMware、华为公有云、华为私有云、微软公有云共 5 个平台。通过部署 DeepFlow® 采

集器、控制器和分析器三大组件，帮助万翼科技在混合云环境中实现了虚拟网络流量的统一采集和实时分析，实现对业务关键链路的全面性能监控，并提供虚拟网络端到端的路径诊断。

- 采集器运行于万科 5 朵云的计算节点，通过从控制器获取 ACL 规则，提供对万科云环境中的网包数据完备的采集和预处理能力（如过滤、分发、Flow 生成、Flow 截取、脱敏等功能）可精细地实现对万科云网络流量的采集和分析。
- 控制器组件以集群模式旁路部署在万科云本地资源池的标准 x86 服务器中，提供万科 5 朵云的对接和全部采集器的管理以及采集策略的管理。
- 分析器组件部署方式和控制器相同，提供丰富的实时分析和回溯取证等功能，并根据项目规划要求，支持横向扩展。

3.2. 部署实施

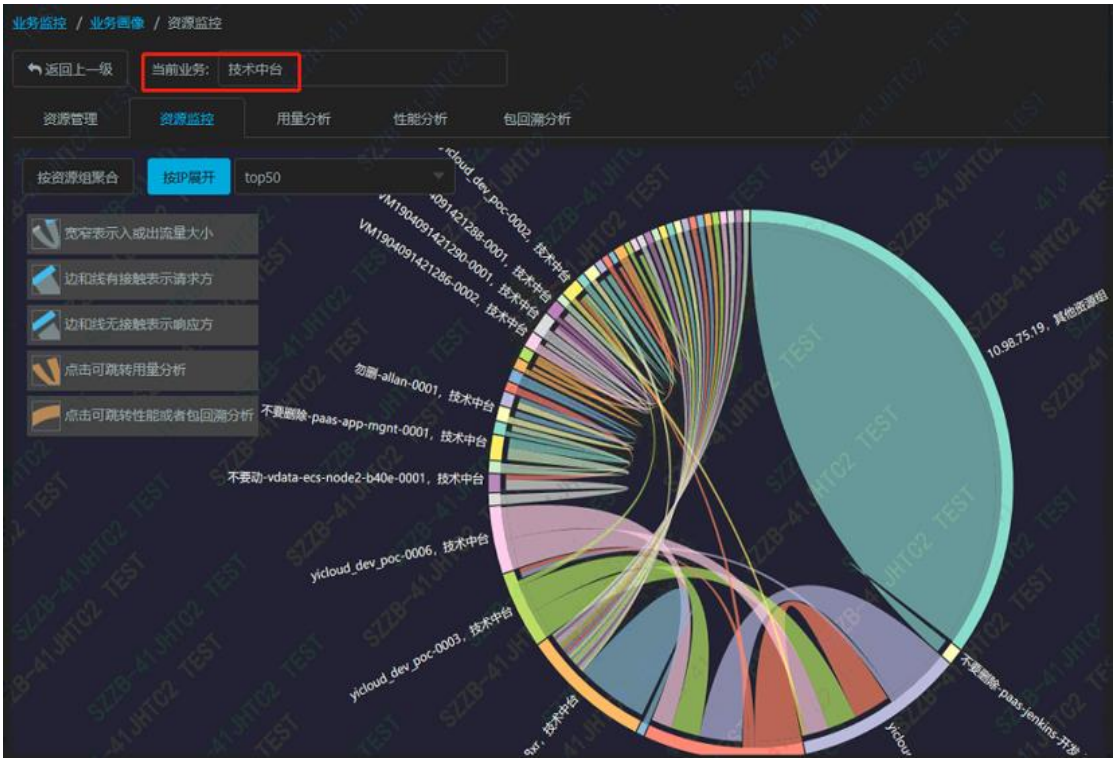
在项目实施过程中，控制器和分析器旁路部署在万科云本地资源池的 x86 集群，控制器通过对接万科云平台实现了虚拟机迁移感知，从而实现了采集策略的自动化跟随；同时 DeepFlow® 拥有对自身系统的全面监控能力，以确保平台稳定运行且不会对万科云环境造成影响。根据万科 5 朵不同云的技术差异，采集器组件在不同的云环境中，采取了如下部署方式：

1. 在基于开源 OpenStack 云平台环境（如华为私有云）中，采集器以用户态进程的形式安装在宿主机上，利用宿主机操作系统自身内核的功能模块，对其虚拟网卡进行流量采集。
2. 在 VMware 云平台、微软 Hyper-V 虚拟化环境和其他公有云中，通过在独立虚拟机中安装采集器的方式，借助宿主机或公有云操作系统自带的虚拟交换机功能实现流量的采集。

3.2.1. 云网全景图

万科云平台对资源上下级的关联展示有所缺失。例如网管平台只有宿主机与虚拟机的信息关系，而云平台又只有 VPC、子网、虚拟机信息；当宿主机故障时，无法判断影响了哪些客户的哪些资源。借助 DeepFlow® 资源拓扑既能查看资源的所有云平台信息、流量统计信息，又能根据不同视角来查看资源的关联关系；例如 VPC 视角能将 VPC 关联的虚拟网关、VPC 所包含的子网、虚拟机、虚拟路由器、虚拟安全组、外网/内网 IP 等全部呈现。

现有的流量统计和管理工具中，基本具备对单资源点的监控，但多资源之间的流量走向关系却不能直观地可视化，因此则不能进行带宽资源优化，也不能监控流量到底流向何方。



借助 DeepFlow® 流量拓扑能力，万科云平台的运营者不仅能从大范围到小范围层层深入揭示流量拓扑关系，也能窥见资源与资源之间、资源与 Internet 之间、资源与未知流量之间的关系。

3.2.2. 云网诊断

云时代东西向流量占比越来越大，虚拟网络越来越得到重视，但虚拟网络问题的定位还处在蛮荒期，多数场景下都是一边人工查看配置信息，一边找到对应设备，一边导流量分析的状态。云平台运营者无法准确知晓业务部门提出来的带宽需求是否合理；也不知道虚拟机的投放是否符合业务需求；不清楚东西向的流量与南北向流量的变化；难以区分哪些业务的流量产生了异常；不能预判活跃 TCP 端口是否有变化。

流量速率

并发连接数

新建连接数

新建连接RTT延迟

系统响应时间

应用响应时间

万科的 5 朵云不同程度地遇到了上述问题，要解决上述问题需要先解决东西向流量带来的巨大压力。DeepFlow® 依靠精准的流量预处理能力，从多资源维度、多租户视角、多流量场景、任意时间粒度来统计与分析云网流量、包量，针对业务画像梳理出来的业务做可视化监控。

此外，DeepFlow® 提供了丰富的可自定义告警设置，万科通过对不同的云资源池、设定详细的网络性能监控指标和告警阈值，从而实现了快速发现和定位业

务网络异常；结合支持五元组采集过滤的 PCAP 下载功能，满足了故障回溯取证的需求，覆盖了故障事前预警和事后分析的全场景。

4. 价值总结

在不侵扰生产网络、不影响业务连续性的前提下，DeepFlow® 通过与万科多云平台的对接，在层次复杂的虚拟网络环境中从服务和应用角度，梳理并监控业务网络，通过对网络指标的异常信息进行实时分析，为业务在虚拟网络中的运行状态提供及时的监控告警。万科云通过部署 DeepFlow® 实现了异构云资源池虚拟网络流量的按需采集、统一管理，解决了多云环境下虚拟流量的一体化管理和分析，为万科集团的业务整合、资源打通和基础设施建设打下了坚实的基础。

了解更多信息

专业的售前技术支持及商务合作，协助您选择最合适的解决方案

详询：400-9696-121

网址：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