云杉网络

看云网更清晰
www.yunshan.net

DeepFlow® 云网分析

国泰君安证券
提升云管控能力和云资源利用率

一. 云管控的重要性

金融云承载业务后，不能仅停留在资源池的建设上，网络是有效实现金融云整体管控重要的一部分。在云中，网络的管理涉及到物理网络层、网络虚拟化层、逻辑网络层等多个层面，而传统的网络管理手段仅涉及到物理网络层，主要针对网络交换矩阵，防火墙、负载均衡等有完整的运维管理方案，但对直接承载业务的逻辑网络的管理仍是一个业内亟待解决的新难题。

规模及异构

随着对业务部、租户服务落地，云资源池通常在一个可用域（AZ，Availability Zone）内，会有 100-400 台计算节点，存在几百个虚拟交换机；在整个云建设中，按照功能角色分区测试云、生产云、公有云等模块；单一类型的资源池并不是企业混合云的最优选择，通常涵盖 VMWare、Openstack、容器、裸金属等资源池。在此环境中，完整获取网络流量就是首要解决的问题。

集中式与分布式

在云环境中，集中单点处理网络流量数据不是一个好的选择，会导致性能瓶颈。为提供对业务的服务保障，需要对云网完全掌握，打开虚拟网络“黑盒”，需

要选型先进的技术架构，对所获取云网内南北向、东西向流量进行处理、分析。分布式的处理能力需要应用到其中，根本上克服单点故障、实现横向扩展并避免高额投入。

排障定位

对快速运维排障而言，单一地分析网络流量在云网环境中是远远不够的。云管信息、虚拟机信息、配置管理信息、部门租户信息等等都要关联至现网流量、并且有能力对物理交换矩阵、网络虚拟化、逻辑网络进行映射，第一时间判断问题所在点迅速协调进行排障应对。

安全

云内网络安全对于生产业务是不能回避的问题，通过安全策略实现业务逻辑网络安全隔离后，业务数量增加、策略数量也随之增加，通过现网流量对已有策略的验证以及异常、突发流量的分析，方可实现在云内庞大网络环境下发现安全隐患的能力。

二. 云流量采集分析是云管控的重要手段

云网监控系统是整个业务安全生命周期中的重要一环，可以事前及时预警发现故障，事后提供翔实的数据用于追查定位问题。一个稳定、高效的监控系统需要具备强大且灵活的数据采集能力。数据中心传统物理网络的流量获取主要通过分光、镜像方式解决，但无法满足和应用于云网络。平台化解决云网流量采集难题，需要满足以下几点：

避免对生产环境侵扰

物理链路分光方式无法采集到虚拟交换机内的网络流量，如果对虚拟交换机直接配置镜像策略进行流量获取，将会直接导致生产数据包转发性能下降。作为生产数据平面虚拟交换机，通常已经由 SDN 控制器配置了大量的生产转发策略，所配置的流量镜像策略有可能与转发策略冲突，存在造成生产事故的风险。此外，SDN 控制器在下发策略配置时，有可能清除所有策略，导致流量镜像失败、监控平面与生产数据平面界定不清晰等问题。

对监控系统负载的管控能力

云网流量采集系统需分配及限定每一个采集器的资源占用，保障生产平面的资源配给，当监控负载过高或超限时，不影响生产环境的交换转发。在混合云环境中，面对几百上千台宿主机的规模，有统一的控制器对流量采集进行管理控制，并应对虚机迁移后的采集策略跟随变更。

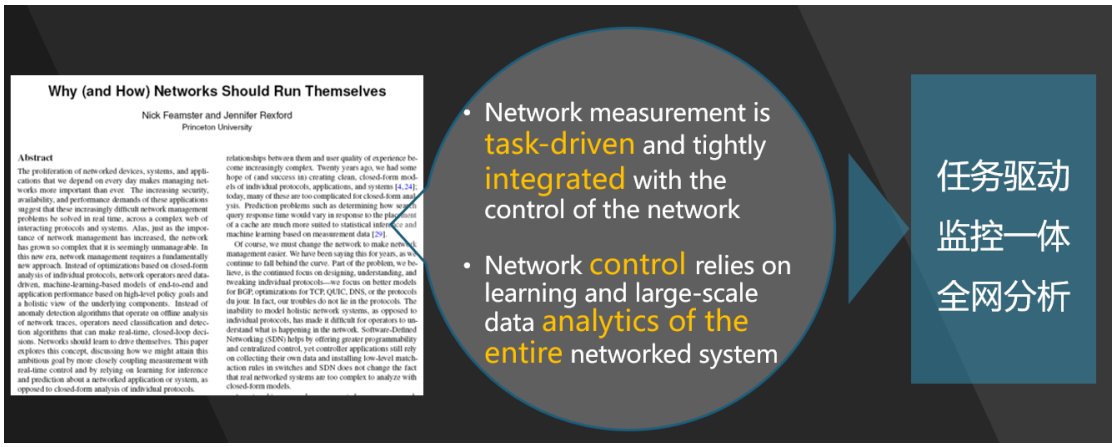
对监控数据包细粒度的管控能力

完全地不加选择地进行全网数据包采集是不合理的方案，会造成存储资源浪费以及针对性问题的检索分析困难。根据业务的重要性，对其监控也有所侧重。在运维监控体系的设计中，重点业务需要保证一定周期的原始数据包留存，非重点业务可以仅保存网络元数据或者数据包报头信息，并有能力进行打标签及数据汇聚。在采集平台中，具备对宿主机、IP、业务资源组、虚拟机等维度过滤，并且有去重、截短、取元等预处理能力。

三. 金融云网络数据运营平台

对于金融云的整体管控，国泰君安并不仅仅是以简单的运维工具视角来规划，而是以整体云数据中心智能化来进行设计规划。以数据中心未来发展的眼界建设整体网络数据平台，并有效解决现阶段混合云运维运营问题。Network

control relies on learning and large-scale data analytics of the entire networked system [1]。



目前金融云网络数据平台基于云杉网络 DeepFlow®已完成建设，具备对混合云网络流量管理、运维排障支撑、开放对接等能力。

平台化、系统化全网流量采集

对数据中心互联网接入线路、专线线路、云内逻辑网络进行全网流量采集，包括 VMWare、Openstack 等多数据中心资源池。有控制器能统一控制千数量级的采集点，并实现对重点业务所涉及流量 30 天数据包留存查询、全网网络元数据回溯能力，每个采集器资源开销仅占用 1 核 CPU 和 2G 内存。

高性能时序数据库

基于网络流量时间序列数据的特点，关系型数据库、对象数据库无法满足对时间序列数据的有效存储与处理，平台基于高性能、可扩展时序数据库对网络流数据进行存储并提供查询能力。

全网可视

虚拟网络不再是运维“黑洞”，云网全景图基于现网流量，绘制资源视角、地域视角、业务视角的流量拓扑视图，关联云平台、部门租户、配置管理信息，快速定位逻辑网络、虚拟机网络故障。

精细化运营

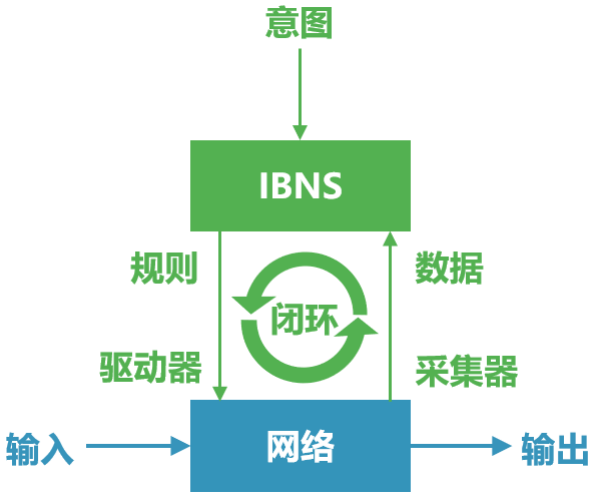
网络不再与业务割裂，资源组定义业务所使用的资源集合，通过网络流量以及业务端口绘制业务热点视图，为运营部门对网络资源调度、计算资源回收提供科学依据。

开放能力

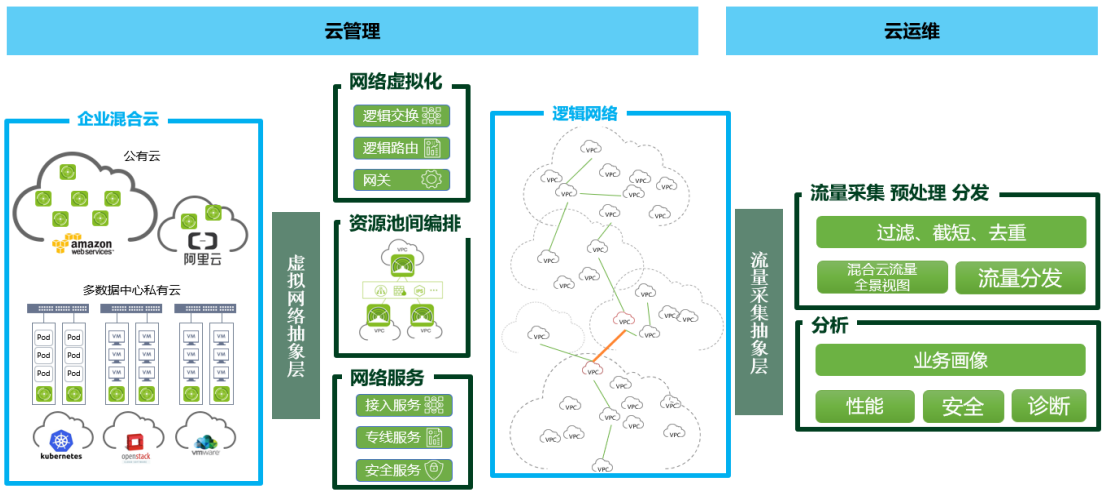
DeepFlow® 控制器支持 Openstack、VMWare、容器等私有环境，同时可扩展支持阿里云、腾讯云、AWS 等公有云环境的部署，支持后续混合云建设扩展。同时 DeepFlow® 秉承了开放可编程的特性，北向提供标准的 Restful API 接口，为数据中心整体大数据平台提供网络流量数据支持及扩展。

四. 金融云后续展望

建设智能化云数据中心是国泰君安的目标，以应对未来更加丰富的证券行业业务、提升管理效率，保障平台可靠稳定。网络做为基础设施的重要组成部分，在未来的发展过程中，必定更加复杂，规模也将超出单纯靠人力运维的能力范围，更全面的自动化乃至基于意图的网络系统（*IBNS：Intent-based networking system*）是可预见的网络未来。Network Automation, Prof. Jun Li, Tsinghua Univ.【2】



在国泰君安的云实践中，网络编排、网络服务与网络数据平台是云网建设的整体框架（如下图所示），避免割裂并保持同步推进。



网络管控方面建设云网互联和服务平台，实现控制与编排解耦，北向为私有云管理平台提供单一资源池网络虚拟化、跨多资源池网络编排能力，南向适配各类交换矩阵，通过建立边界服务资源池，为私有云平台提供网关、防火墙、负载均衡等网络服务。网络监控方面持续完善云网数据平台，将广泛扩展至整体数据中心，并针对性的将网络流量分发至更丰富的工具链及数据消费部门，在审计、安全等方面提供完整的数据服务。

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