云杉网络

看云网更清晰
www.yunshan.net

DeepFlow® 云网分析
民生银行容器网络监控实践

一、 业务大量上云与应用架构变迁

在过去数年里，在十三五规划指引下，金融行业通过私有云、行业云、生态云的建设以及大力发展金融科技的战略，已经成为上云的领航者。目前各金融企业正在大力建设基于容器和 K8S 的云平台，用于快速部署或迁移发展迅猛的生产应用。

民生银行作为国内领先的金融企业，在上云的道路上进行了广泛的探索，较早地认识到容器轻量化、标准化、弹性、可移植、高效发布等好处。目前已建设了自己的应用容器云平台并在全面推广使用中。随着民生银行应用的容器化，创新类应用得以快速上线、快速迭代；传统的应用借助容器加速了 DevOps 和微服务改造，业务在部署和调度方面的效率得到了大幅提升。但容器的引入再一次扩大了云网络的边界和层级，随之而来的监控问题也摆在了桌面上。

二、 民生容器云平台

容器轻量化、标准化的特性降低了管理的复杂度，满足了业务大量上云的需求。随着 Kubernetes 赢得了容器编排之争，企业采用容器大多会选择 Kubernetes，容器网络方面，在 Kubernetes 官网登记的 CNI 已有几十种。为了解决隔离性和

跨节点的容器通信，Overlay Network 成为众多企业建设容器网络方案的首选。民生银行容器云平台也是基于 Kubernetes 和 Docker 技术构建，容器网络采用了 Flannel+Overlay 模式。网络部门一直肩负着业务统一管理和发布的重任，并随着云计算和 IT 技术的发展建设了完善的网络监控平台。但容器业务的监控涉及注入负载均衡等网络设备、Kubernetes 池内的 Service 资源以及 Ingress 资源，并且容器的原始网络模型对多租户或者说业务隔离的体制并不完善 ,这都为容器业务的监控带来了许多新挑战。

三、 云原生的监控网络

容器环境中的常见故障一般有三类 :应用类故障通常表现为应用的执行状态和预期不符；容器故障通常表现为无法正确的创建、停止或更新容器；集群故障通常表现为不满足一致性或无法连接。多数企业在容器部署及管理方案中，对系统监控报警多采用 Prometheus、Grafana、Zabbix 等开源工具，但所能获取的指标数据和展示维度相对有限，尤其是当容器资源池规模继续扩容后，上述工具的扩展性和部署问题将难以满足深入的分析需求。以容器 Host 模式为例，通常每个节点运行 100~200 个 Pod，获取每个 Pod 的网络流量并结合全网流量数据，实现秒粒度的查询分析并不容易。

获取完整的网络流量尤其是容器网络的流量是保障业务上云连续性和安全性的重要前提。在容器云平台中，业务与网络的结合更为紧密；在容器云平台内部，默认的网络模型在东西向访问隔离方面缺少必要的安全保障；在微服务架构中，服务间的网络监控是业务保障中重要部分；在容器网络中，POD 间的网络流量迫切需要工具手段进行监控保障。民生银行构建了统一的云网络监控平台，具备

满足业务上云持续演进的能力，确保业务上云后的可视、可管、可控以及快速排障。这就要求对容器业务的监控能够识别到 Pod 粒度，能主动感知容器资源的变化监控手段也应随之改变。借助开源组件和商业产品如云杉网络 DeepFlow® 等，民生银行的监控平台实现如下目标：

1. 安全可控：在容器环境下，满足平滑部署且容器业务不能间断，对计算资源的消耗可控。
2. 一体化：监控能力覆盖包括容器、KVM、VMware、公有云、裸金属等异构资源池，同时具备多租户服务能力和容器业务的端到端诊断能力。
3. 云原生：监控平台采用分布式架构，满足云服务的弹性、敏捷需求，当容器业务进行跨资源池弹性部署时，监控系统可以自动跟随。
4. 开放性：多类分析终端或平台对容器网络的流量数据有消费需求，确保现有的分析工具可以无缝使用。

企业选择 Kubernetes 构建容器云平平台时，一定程度上解决了管理的便利性问题。但在容器网络方案中却面临着一些不足，尤其是在大规模场景中，容器的网络隔离、地址管理、网络性能以及故障诊断方面存在不足。具体到民生银行的业务场景中，云端业务的发布主要借助蓝鲸系统，网络监控依赖统一的网络数据平台——由前端的 TAP 设备实现各网络和业务环境的全量网络数据采集，通过流量汇聚设备进行流量预处理（包括去重、过滤、复制等），然后分发到后端网络流量分析、安全分析、交易分析等数据消费工具使用。

民生银行数据中心安全和业务规划为多个区域，容器集群部署在多个区域。面对

业务向私有云和容器环境过度中虚拟网络流量采集的不足，借助云杉网络 DeepFlow NPB 方案，首先与各区域的容器资源池进行对接，掌握了容器环境中的相关信息，包括集群（Cluster）、节点（Node）、Pod、服务（Service）、Ingress 等；根据容器环境分别部署对应规格的采集器，采集器获取 POD 原始流量，在业务梳理过程中标定监控对象，并加入相关的资源组、归类 IP、功能服务、链路，描述容器业务的网络访问路径，并根据采集策略为分析工具做流量标记、业务标记，并将标记信息同步到 CMDB 供各类分析工具使用。采集器将资源池内的流量按业务画像梳理出来的规则过滤，并分发到后端各类分析平台或设备，从而实现容器业务端到端的监控与诊断。

四、 云原生监控的展望

当前，容器云在金融行业落地还存在许多问题需要解决，例如容器业务的安全隔离，容器网络与数据中心网络的统一监控等。容器在金融行业的部署规模日益增长，未来应用微服务化、容器化将会是一个主流技术方向。通过进行针对性适配和改造，容器在民生银行的应用将逐渐规模化。但对容器网络的监控仍需要精细化，需要从区域、节点、Pod、IP 等多个维度查询展示容器业务，在容器业务路径中实现分段排查、快速缩小问题范围、定位异常原因；并为回溯取证提供数据支撑。未来，民生银行将持续推进容器网络监控方案持续落地，助力业务创新，践行科技金融战略。

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