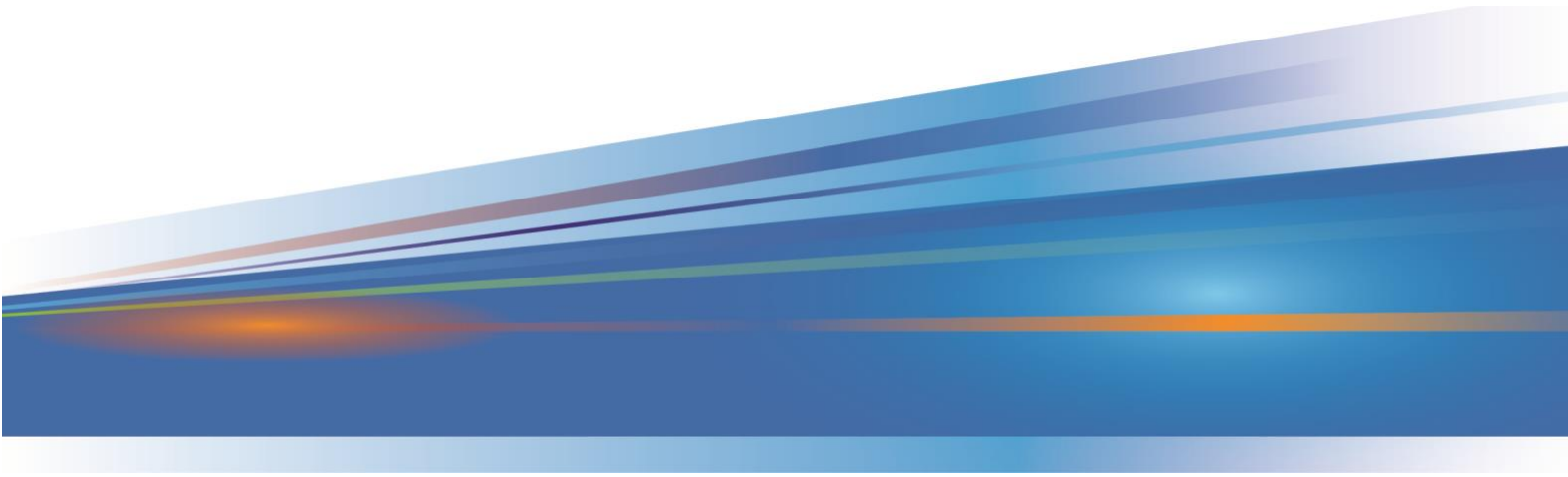
云杉网络

DeepFlow®

5G 核心网网络功能服务监控方案



北京云杉世纪网络科技有限公司

目录

1. 前言

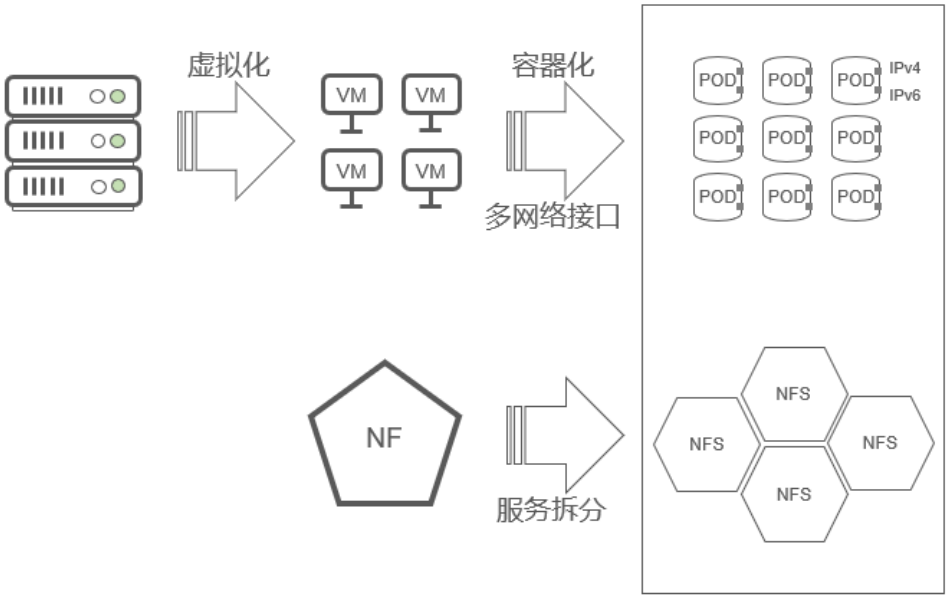
5G 建设推进，深度融合云计算、网络、边缘计算，提供大宽带（eMBB，增强的移动宽带）、低时延（uRLLC，超可靠低时延通信）、广连接（mMTC，海量物联通信）的接入能力，更多地面向企业服务，为工业互联网、车联网、虚拟现实、超高清视频等场景提供垂直应用基础平台。5G 核心网是 5G 建设的重要组成部分，采用全新技术，在实现网络部署、网络功能、新业务开展的同时，监控保障也面临全新挑战。本方案介绍如何面向基于服务架构的 5G 核心网，匹配网络功能服务以具备高效的监控保障能力。

2. 5G 核心网监控面临的新挑战

在 4G 核心网（EPC，Evolved Packet Core）中，网元由专有设备支撑，硬件属性较强。在 5G 核心网（5GC，5G Core），采用的是基于服务架构（SBA，Service Based Architecture），融入云原生、微服务等设计思想， 以软件化，模块化、服务化的方式构建核心网。对于核心网的生产保障，其网络功能（NF，Network Function）及服务（NFS，Network Function Service）间的依赖关系、访问调用、性能追踪都面临全新挑战。主要集中在：

网络功能拆分

依据 3GPP 定义，5G 核心网的各网络功能（NF，Network Function）在功能级别上拆分解耦，拆分出若干个独立解耦的网络功能服务(NFS，Network Function Service)，这些网络功能独立运行，提供标准化服务接口，通过相互调用访问实现网络功能。



图：网络功能拆分

虚拟化、云原生技术的融入，在 5G 核心网方案中，不再大量使用专有硬件设备，取而代之的是通用服务器承载的虚拟网元，虚拟机、容器 POD 数量飞速增长，每个工作负载同时提供多个 IPv4、IPv6 工作平面。

相较 4G EPC，由于众多演进叠加在一起，如图网络功能拆分所展示，在 5G 核心网 SBA 架构中虚拟化后的 NFS 实例数量以 2 个乃至更多的数量级增长，监控对象数量大是 5G 核心网保障侧第一个挑战。

服务自动化管理

通过网络功能仓储*(NRF，NF Repository Function)*，5G 核心网的各类网络功能服务得以自动化管理，实现服务的自动发现以及注册、更新、状态检测等，避免服务访问中进行大量手动配置工作；集中控制面可以将大量跨区域的信令交互变成数据中心内部流量，优化信令处理时延；根据业务应用的变化，按需快速扩缩网络功能和服务，提高网络的业务响应速度。自动化管理在生产侧提升了管理效率，同时也增加了核心网动态性强、难以跟踪的挑战。

通信路径优化与交互解耦

4G 核心网的网元之间有着固定的通信链路和访问路径。例如，用户的位置信息必须从无线基站上报给移动管理单元*(MME，Mobility Management Entity)*，然后通过其发至服务网关*(S-GW，Serving Gateway)*传递给 PDN 网关*(P-GW，Packet Data Network Gateway)*，最

终由策略计费规则功能单元*(PCRF，Policy and Charging Rules Function)* 进行策略更新。网元之间的通信遵循请求者和响应者的点对点模式，是一种相互耦合的传统模式。

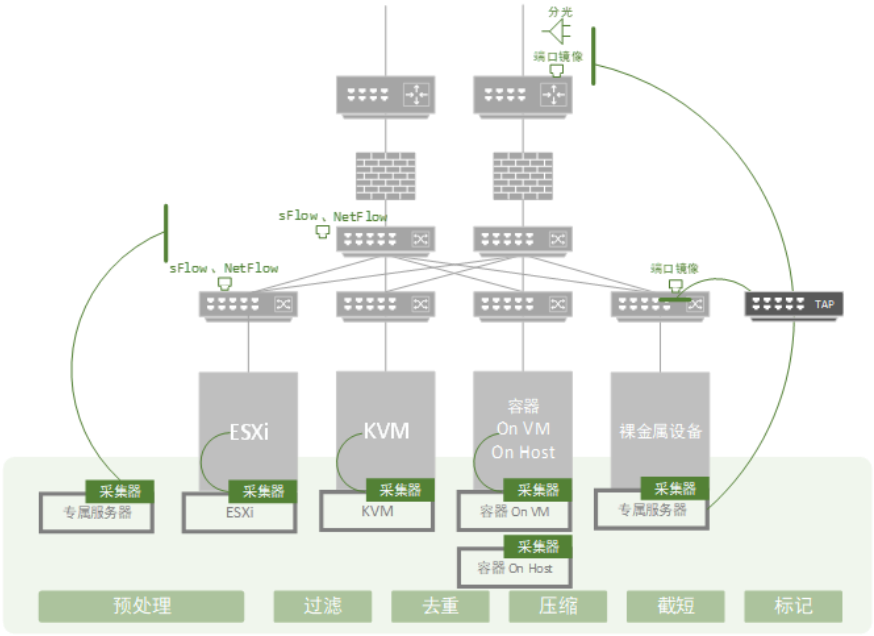
在 5G 核心网服务化架构下，各网络功能服务之间可以根据需求按需通信。5G 核心网架构下的网络功能服务间通信机制进一步解耦为生产者和消费者模式，具备灵活可编排、解耦、开放等优点，是 5G 时代迅速满足垂直行业需求的一个重要基础能力。各网络功能在实际应用过程中，避免了不必要的网络中转同时，但所涉及的调用链追踪，性能分析，故障定位等也成为了新的挑战。

3. DeepFlow®平台

DeepFlow® 是一款面向 5G 核心网，应对网络功能 NF 分拆解耦后的新挑战，基于对服务 NFS 间的通信访问流量进行获取分析，以保障核心网稳定运行的软件产品。产品主要由采集器、控制器、数据节点三部分组成。

采集器 网络流量获取及预处理

在 5G 核心网环境中，由于普遍使用虚拟化及容器技术，获取功能服务 NFS 间访问调用所涉及的网络流日志、数据包并非易事。DeepFlow® 采集器基于分布式架构，实现对各类型资源池以及物理网络的流量采集及预处理抽象层。



图：DeepFlow®采集器

如图 DeepFlow®采集器中，各类型号的 DeepFlow® 采集器为 5GC 运维保障提供基础流量捕获能力，支持物理网络、KVM、ESXi、容器等资源池网络环境，实现采集侧可弹性扩展。详细技术信息可参考云杉网络“混合云全网流量采集与分发方案”。

通常 5G 核心网环境中，主要涉及到 KVM 虚拟机与容器 POD 的网络流量获取，如下图所示。

图：5GC 环境网络流量获取

监控保障框架同样需要弹性可扩展，通过采集抽象层，实现流量获取与后端数据分析实现解耦。流量获取侧主要避免对生产环境的侵入和额外的配置，在 DeepFlow®方案中，采集器以独立进程形式存在，部署在 KVM Hypervisor 系统或者容器 POD 上，无需对 vSwitch 增加镜像策略以及更改系统配置。此外，采集器的工作运行是在预先指定的 CPU、内存等资源范围内，最大限度不影响生产侧。采集器以分布式系统处理的方式对数据包进行过滤、去重、压缩、标记等预处理，避免单点性能瓶颈。

控制器 平台控制中枢

对于 5G 核心网，用户面将逐步下沉以靠近用户侧，边缘云可快速响应处理用户侧请求，减小时延；中心云集中部署管理面和控制面，集中统

一进行管理控制。中心云、边缘云涉及多数据中心、多资源池且分布在不同地区，监控保障平台控制面需要解决所面临的多点多地的问题。

控制器是整个 DeepFlow®平台的控制中枢，统一管理各类采集器及数据节点。控制器集群实现对平台的管理控制平面的扩展，分为主控制器、备控制器、从控制器，可按照部署要求进行选择，为平台提供统一的控制接入点。单一控制器最大支持控制管理 2000 个采集点，控制器集群可扩展至 50 台主、备、从控制器，管理 10 万级采集器能力。

主控制器：整个 DeepFlow®平台的控制中枢和提供对外交互、服务的接口。部署后的 DeepFlow®平台中只有一台主控制器，主控制器所在的区域称之为主区域。

备控制器：与主控制器的功能完全一致，当主控制器出现宕机或不能提供服务的其他故障时，自动切换为主控制器。在没有备控制器的情况下，DeepFlow®控制器集群没有高可用能力。整个 DeepFlow®中只有一台备控制器，且必须和主控制器在同一个区域中，并共享一个用于提供外部服务的虚 IP 地址。

从控制器：负责控制所在区域（*Region*）或可用区（*AZ，Available Zone*）中的采集器及数据节点，将主控制器的策略和云平台资源信息同步至所有的采集器和数据节点。除主、备控制器所属的区域，每个区域中

至少部署一台从控制器，同一个区域的多台从控制器之间可以实现负载均衡和高可用。

在多点的部署环境中，首先指定主区域（Region），主控制器存在于主区域中，当启动主控制器高可用功能，主区域内应部署多台控制器，通过心跳保证控制器间的状态同步，及时启动主、备控制器选举。选举产生主控制器后，为整体流量管理平台提供控制入口。除主区域外的其他区域控制器为从控制器，不参与主控制器选举。

在区域中可以划分多个可用区（AZ，Available Zone），通常以可用区为单元，由单一控制器独立控制可用区内的各类型采集器，对本地采集器进行采集策略、分发策略、预处理策略下发。多区域间可通过专线网络进行控制通信，主要包括管理、策略等通信。

数据节点 高性能网络时序数据库

网络功能服务 NFS 间的调用流量是典型的时间序列数据，同时具备相应的网络特性。满足服务调用链监控追踪要求，需要具备对所存储的网络指标数据进行分组聚合，提供高性能查询能力，展示访问调用性能趋势、规律、延时、异常等。数据节点核心是分布式时序数据库，为平台提供时序数据的快速写入、持久化、多纬度的聚合查询等基本功能。

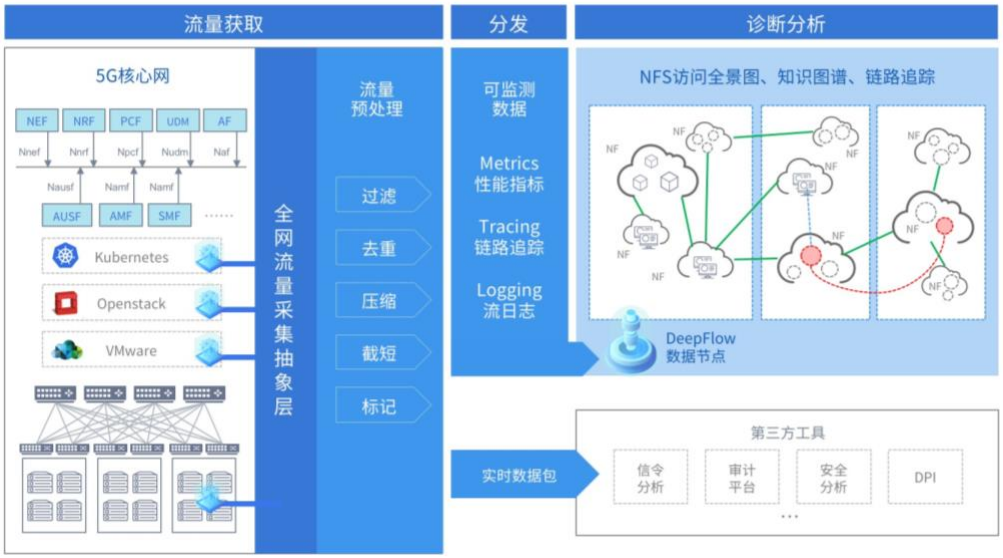
时序数据库（TSDB，Time Series Database）是用于存储监控数据的专用数据库，通过对监控数据在时间维度上的压缩存储降低写入开销。

写入特征：由于网络通信的端到端特性，一个万台服务器的环境中产生的系统监控数据每秒写入量级为 O(N)，但每秒产生的网络数据取决于相互通信的服务器数量，极端情况下可能达到 O(N^2)。若将通信时的协议、端口号也进行记录，还会导致监控数据对象进一步升高，因此用于记录网络监控数据的时序数据库所需具备的首要特性是亿级别数据对象的支持能力，此外，云环境中所固有的弹性也要求时序数据库需要支持弹性伸缩。

查询特征：除了常规的查询某个 IP 地址以外，对 5G 核心网网络功能服务监控还要求能从各种维度进行查询，这需要对监控数据添加不同维度的属性。例如资源池维度的区域、可用区，虚拟化维度的宿主机、虚拟机，容器维度的节点、POD、Service、命名空间、资源组等。在动态性强的服务调用过程中，也要求运维排障不能再依靠总量、峰值、均值等简单的统计数据，时序数据库应当提供更丰富的指标量计算能力，如中值、概率分布、信息熵、方差等。

4. 5GC 网络功能服务监控方案

本方案的目标是为 5G 核心网建设可扩展的网络功能服务 NFS 监控平台，应对功能拆分解耦后各类资源间网络性能分析，支持 IPv4、IPv6 协议环境，紧密结合 http v2 协议，实现服务间关联依赖监控。整体方案由上述 DeepFlow®的采集器、控制器以及数据节点组成。



图：5G 核心网监控方案

在整体方案中，可按处理逻辑分为流量获取、数据分发传输、诊断分析三大部分。在流量获取部分，由各类型采集器承担，主要提供高效、可管理的服务 NFS 间访问调用流量的捕获能力。分布在多区域的各类型采集器由控制器统一管理，下发采集、分发策略。通过流量采集预处理抽象

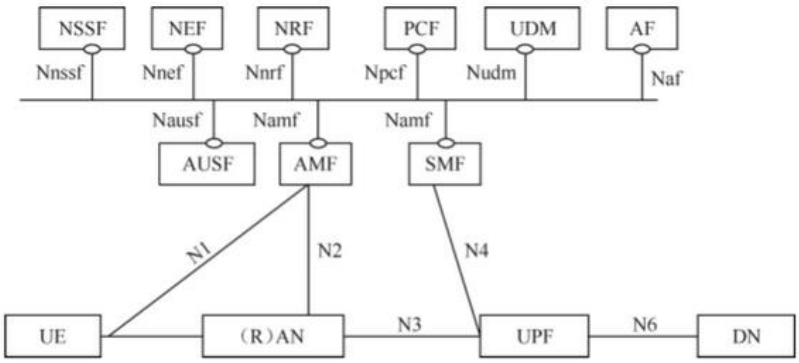
层，提供流量采集及预处理的北向管理接口，使整个监控平台具备可扩展的基础数据获取能力。

获取到流量数据后，下一步就涉及到数据分发传输部分。为了保障监控方案的全面及扩展性，获取到的流量数据可分发至 DeepFlow®产品的数据节点以及第三方的分析工具中，保障对数据分析消费的多样性。从分发角度看，需要着重考虑传输数据所占用的带宽及效率。DeepFlow®数据节点主要收集存储服务间访问的指标数据、流日志，与完整的数据包数据相比，指标数据在传输过程中达到 10000:1 的压缩比例。与此同时，平台可以根据实际需求，配置分发策略，分发完整的数据包或截断后的包头数据。

在数据消费分析侧，DeepFlow®数据节点提供面向 5GC 服务的分析能力，核心目标是向运维保障人员提供全网知识图谱、服务 NFS 访问全景图、全栈跟踪、告警报表等功能。通过第三方分析工具的扩展整合，可以完整覆盖深度包检测*（DPI，Deep Packet Inspect）*、信令分析、安全审计等场景。

全自动绘制知识图谱

5G 核心网中，网络功能是性能监控保障的核心，整个核心网通过虚拟化以及服务化后，除关注各类型的网络功能外，还涉及各云、容器等不同维度。绘制一张多维度的知识图谱是服务监控的核心能力，通过关键实例快速查询关联信息。如图基于服务化的 5G 核心网架构中，包含各类型网络功能以及用户设备（UE，User Equipment），无线接入网络（RAN，Radio Access Network），数据网络（DN，Data Network）。



图：基于服务化架构的 5G 核心网

在核心网中的主要网络功能，主要有：

应用功能（AF，Application Function）

接入和移动管理功能（AMF, Access and Mobility Management Function）

认证服务功能（AUSF，Authentication Server Function）

网络开放功能（NEF，Network Exposure Function）

网络存储库功能（NRF，Network Repository Function）

网络切片选择功能（NSSF，Network Slice Selection Function）

控制策略功能（PCF，Policy Control Function）

会话管理功能（SMF，Session Management Function）

统一数据管理功能（UDM，Unified Data Management）

用户平面功能（UPF，User Plane Function）

网络功能通过容器 POD 或虚拟机承载实现，在生产运行过程中，网络功能与拆分后的服务实例其属性涉及多个维度，DeepFlow®平台通过对云平台（如 Openstack）、容器平台（如 Kubernetes）进行 API 对接，主动学习环境中的相关信息，包括：

资源池：

区域（Region）、可用区（AZ，Available Zone）、平台

虚拟化：

宿主机（Host）、虚拟机（VM，Virtual Machine）、路由器、安全组、NAT 网关、负载均衡器、RDS、Redis 等

容器：

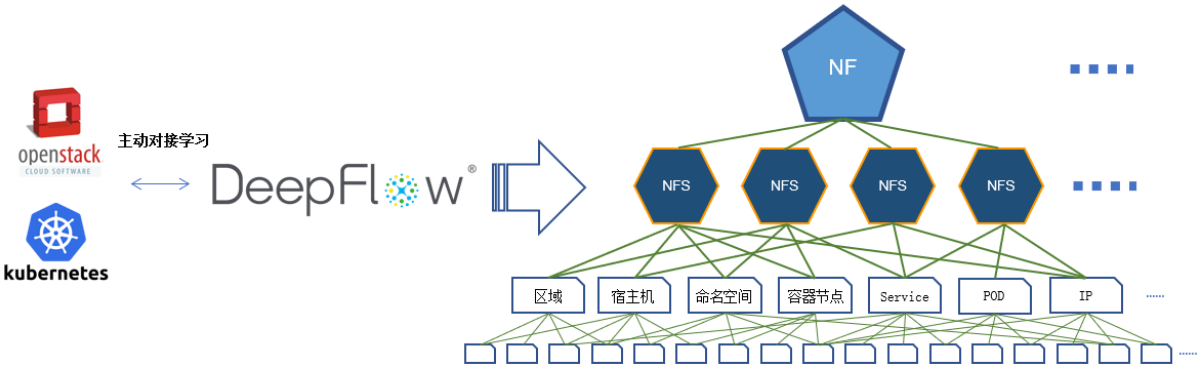
容器集群、命名空间、容器节点（Node）、容器 Pod、Ingress、容器服务（Service）、工作负载、ReplicaSet

应用相关：

网络功能，资源组

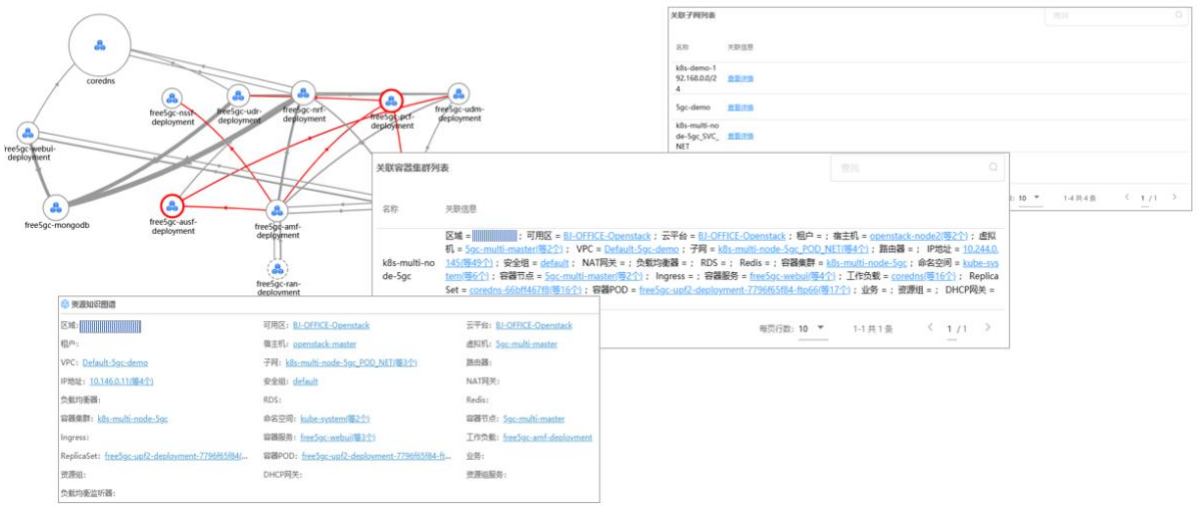
网络：

IP、VPC（*Virtual Private Cloud*）、子网



图：知识图谱

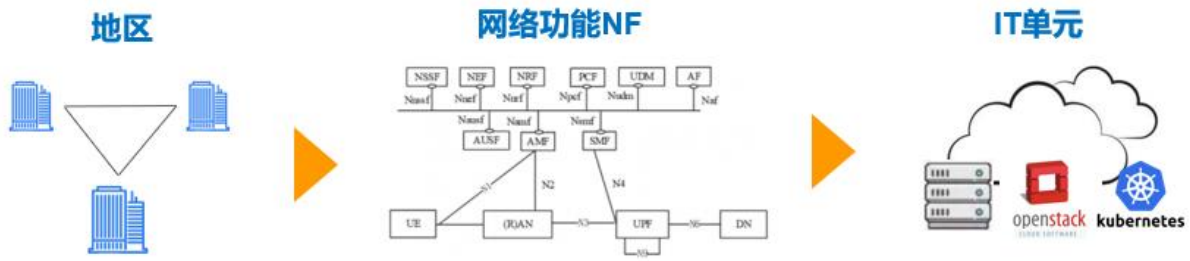
在“知识图谱”功能中，可以针对关注及圈定的实例，快速跳转、关联相关维度的实例及详细信息。如下图示例中，在众多网络功能中，当需要确定延时热点 AMF 功能所关联的多维度信息，定位其区域、集群、节点等。反之，也提供快速关联属于统一集群、节点等的服务、POD、IP 等信息。知识图谱是 DeepFlow®平台实现更丰富的监控保障功能，提供信息管理、跟踪跳转的核心能力。



图：知识图谱示例

由大到小看服务

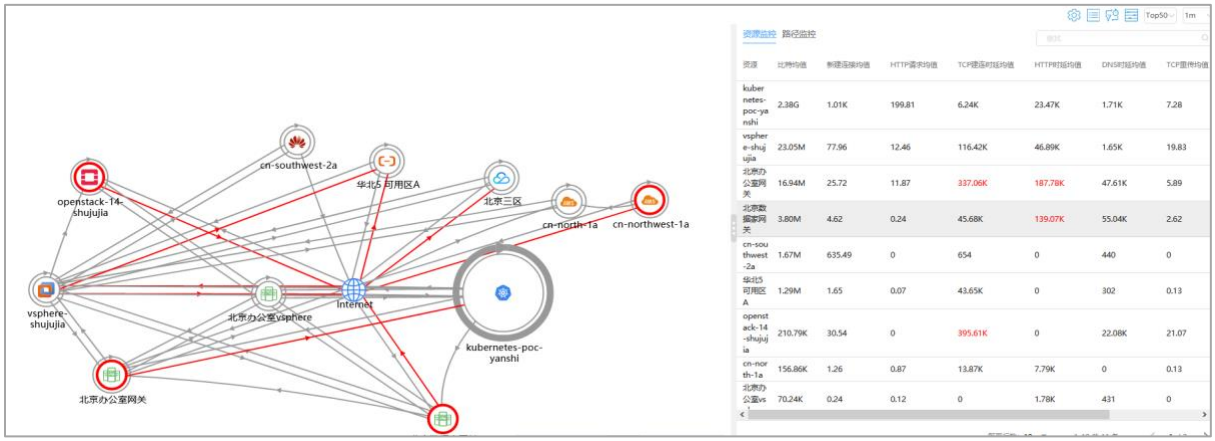
全景图功能为 5G 核心网保障人员提供由大到小，逐级有序的服务运行状态视图展现。



图：全景图

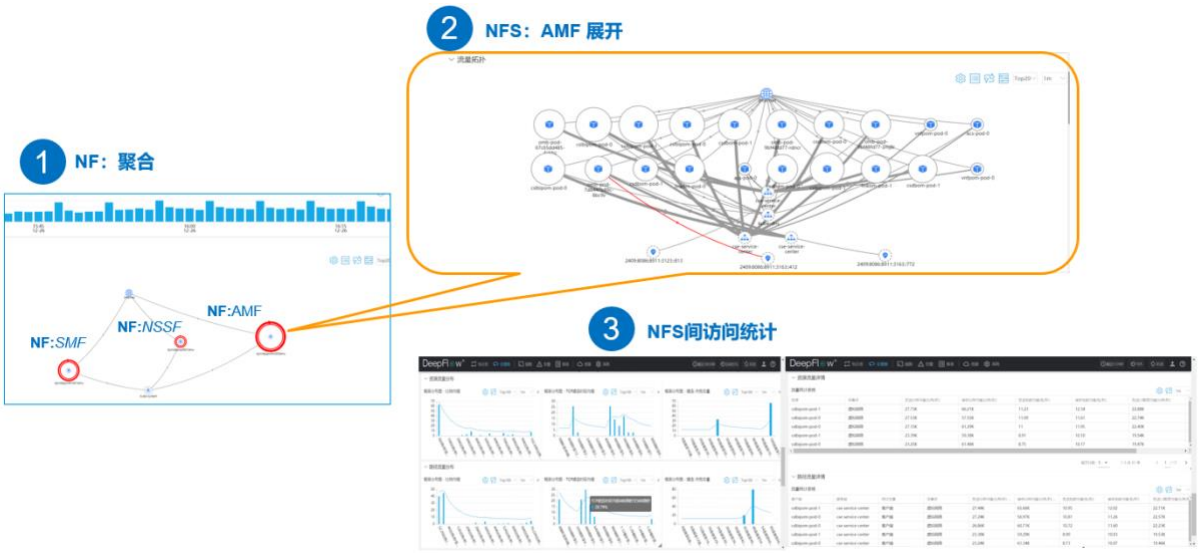
在 5G 核心网的监控实践中，通常根据工作流程分为三大范围，较大范围以数据中心所属区域或资源池划分，其次为网络功能或服务类型，比如 AMF、UDM、SMF 等，最后将集中在 IT 单元，比如容器 POD、宿主

机、IP 等。DeepFlow®平台按照三类范围由大到小的操作划分，为核心网所涉及到的复杂网络提供完整的、逐级的监控跟踪。



图：全景图地区示例

对于多地资源池，在区域视图中，汇总可用区、资源池中的性能指标进行展示，从整体视角快速掌握整体状态。以 5G 核心网网元功能为视角，同样可以快速展现功能、服务间访问调用的依赖关系及各类性能指标。



图：全景图功能服务示例

如图全景图功能服务示例，第一步操作，以相同 NF 为单元进行聚合，展示 NF 整体的性能状态及访问关系，逐级展开拆分后的各类 NFS 间的访问调用。在第二步操作中圈取展开 AMF 功能中的所有服务间的关系及性能。当需要获取更详细具体的指标统计信息时，可以直接列举或展示相应图表，在图中第三步中就是选取了相应的服务 NFS 访问通信对进行分析对比。

图：全景图 IT 单元示例

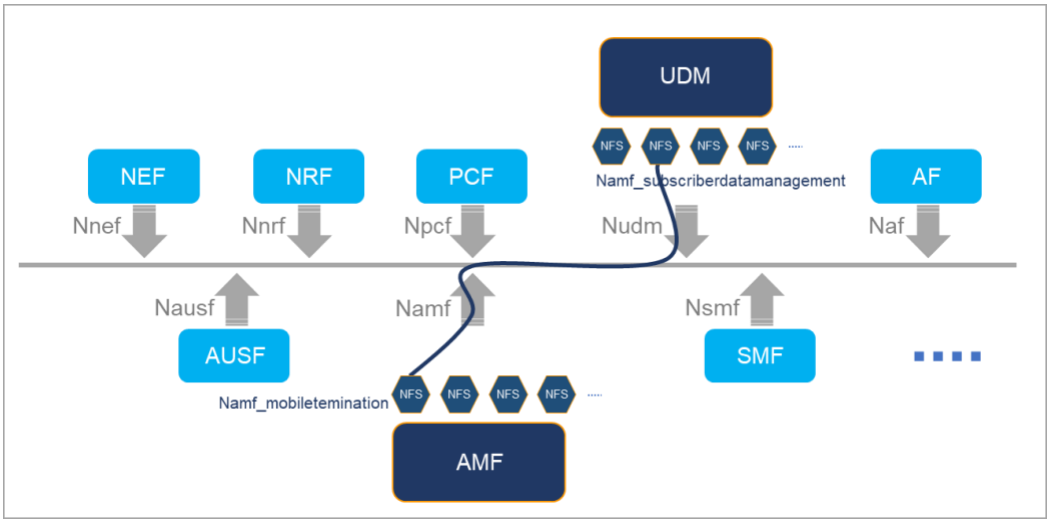
当观察到异常或者希望检索特定服务实例时，如图全景图 IT 单元示例中，在服务调用应用延时分布图中，存在近 18%的 5 秒高延时访问调用，需要关注其网络服务的相关 IT 类型、属性、性能指标等。平台可以迅速展开高延时访问所涉及的服务和 IT 资源信息，以及相关的访问关

系、性能状态。深入细节分析原因时，可以通过抓取数据包功能，获取指定范围的完整数据包。

DeepFlow®平台提供强大的指标数据能力，针对不同维度的访问关系对，端到端性能等提供 12 类 110 种指标量，与算子结合可产生 1170 个指标量统计值。涵盖网络层、传输层、应用层的各类型数据，尤其在 5G 核心网中使用的 Http v2 协议的异常、时延和超时。

分钟级定位异常边界范围

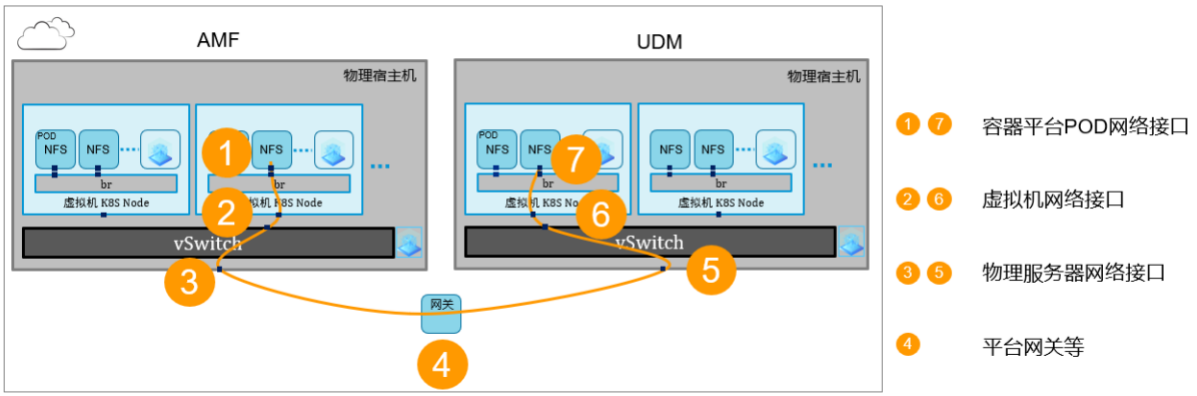
5G 核心网中存在大量的、复杂的 NFS 间服务调用，具备有效的调用性能跟踪能力尤为重要。



图：服务间访问示例

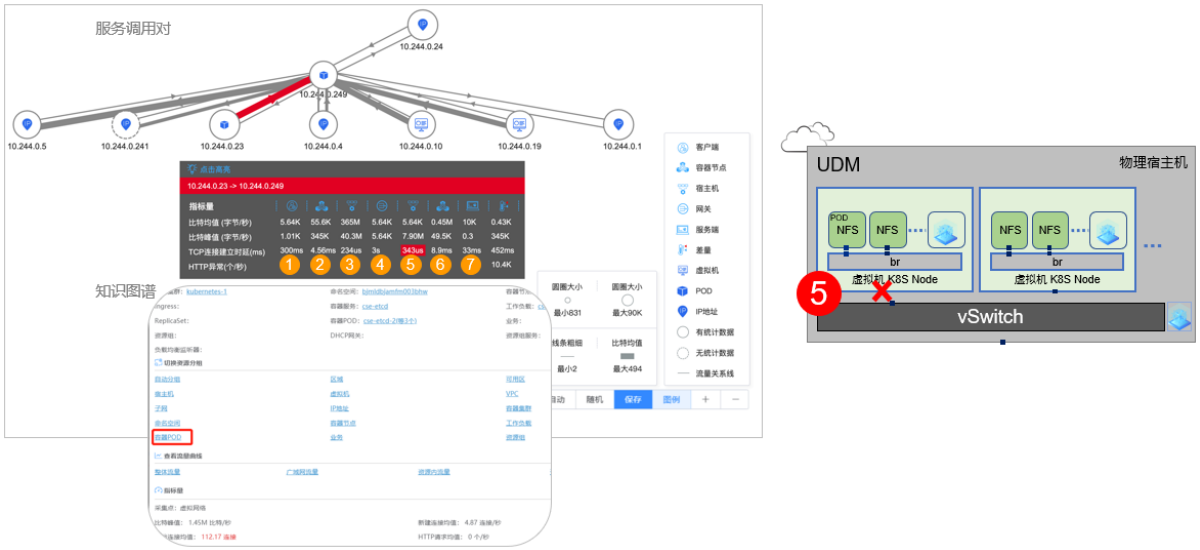
如上图所示，一个简单的逻辑调用，AMF *（Access and Mobility Management Function）* 中的 NFS 调用 UDM*(Unified Data Management)*

中的 NFS 获取用户信息，这个过程中，并不是像传统环境中直观简单。在 5G 现网环境中，普遍涉及宿主机、虚拟机、容器的网络虚拟化实现，以全栈分段来梳理访问调用，是应对新环境运维排障挑战所必须具备的。以全栈视角，展开以上调用，可以剖析 NFS 发起调用所经过的 POD 接口、虚拟机接口、宿主机接口乃至网关等链路。



图：服务调用全栈跟踪示意图

全栈跟踪针对云中服务间的调用访问，将虚拟化所实现的逻辑通信进行逐步展开，清晰便捷展示每段的网络状态，性能，结合知识图谱及丰富的指标数据，快速定位性能异常的问题范围边界。以上所述访问为例，如果排查调用延时故障，确定 NFS 调用服务双端后，展开全栈跟踪，直接定位延时所在的接口。如全栈跟踪示例图中，清晰展示出服务 AMF 服务实例至 UDM 服务实例两端访问延时瓶颈在 UDM 功能侧，且聚焦在其运行所属虚拟机的虚拟网络接口处。而排除 UDM 服务实例的 POD 网络接口及 AMF 所涵盖的虚拟机、POD 等众多接口路径。



图：全栈跟踪示例

在没有 DeepFlow®全栈跟踪工具的情况下，排查服务访问调用的性能将是一个复杂繁琐并且冗长无头绪的过程，同时对于一线运维人员要求所掌握的技术栈较多，综合能力强，很可能耽误宝贵的运维窗口时间。

5. 基于 Free5GC 的示例

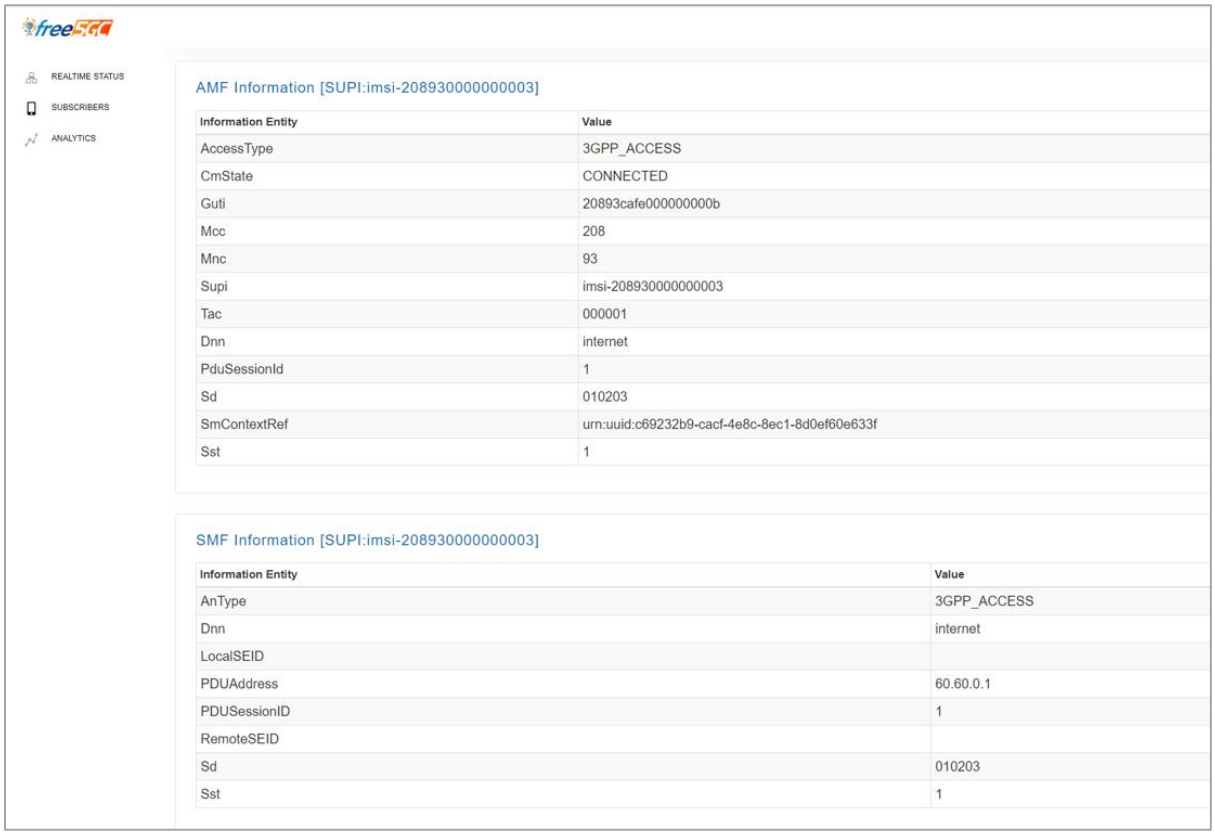
Free5GC 是 5G 核心网开源软件项目，总体架构基于 3GPP 标准、遵循 SBA 框架，采用虚拟化方式实现网络功能，可运行 5G 核心网的标准服务，并且可以模拟相应工作流程。

What is free5GC?

The free5GC is an open-source project for 5th generation (5G) mobile core networks. The ultimate goal of this project is to implement the 5G

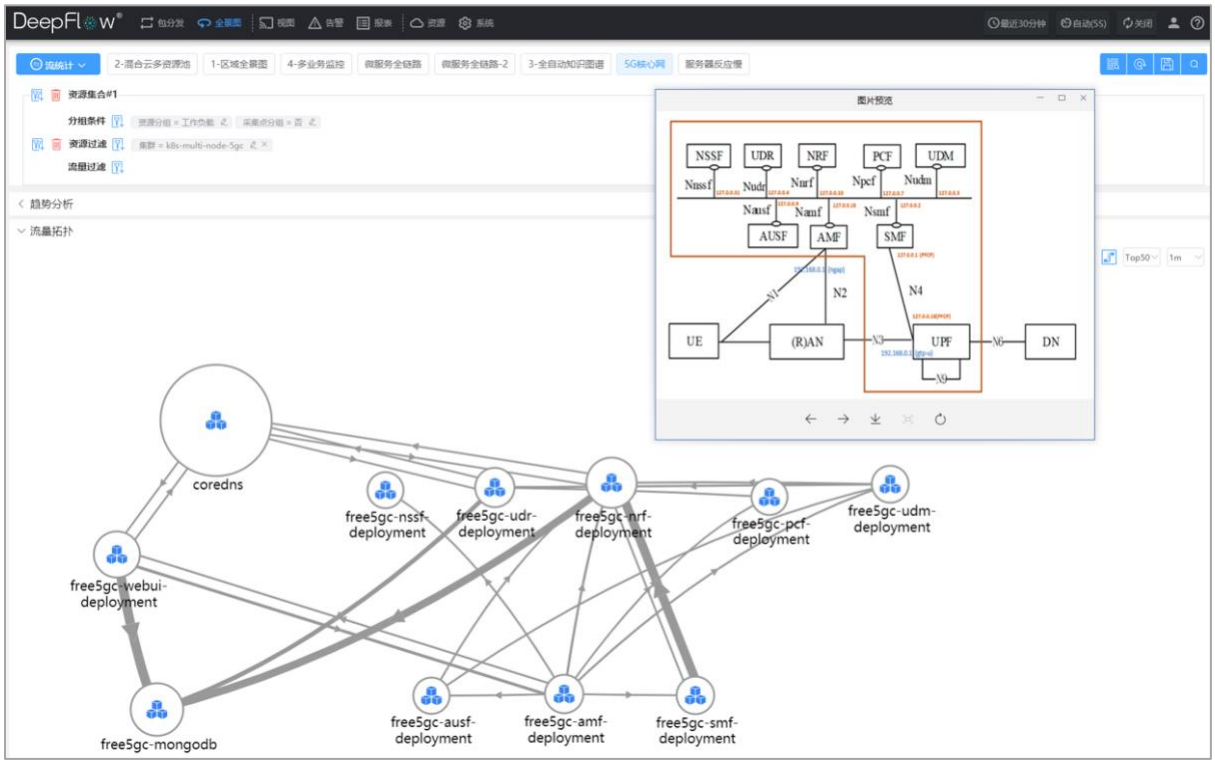
core network (5GC) defined in 3GPP Release 15 (R15) and beyond. -- www.free5gc.org

在实际 5G 环境中，多数厂商已经采用容器技术承载网络功能服务，所以在本示例环境采用虚拟机运行容器，创建 Kubernetes 集群， 搭建 5G 核心网验证环境，使能各网络功能。部署 DeepFlow®平台监控网络功能服务（NFS）运行全景以及服务调用性能，演示全栈跟踪能力。如下图展示模拟用户端注册信息。



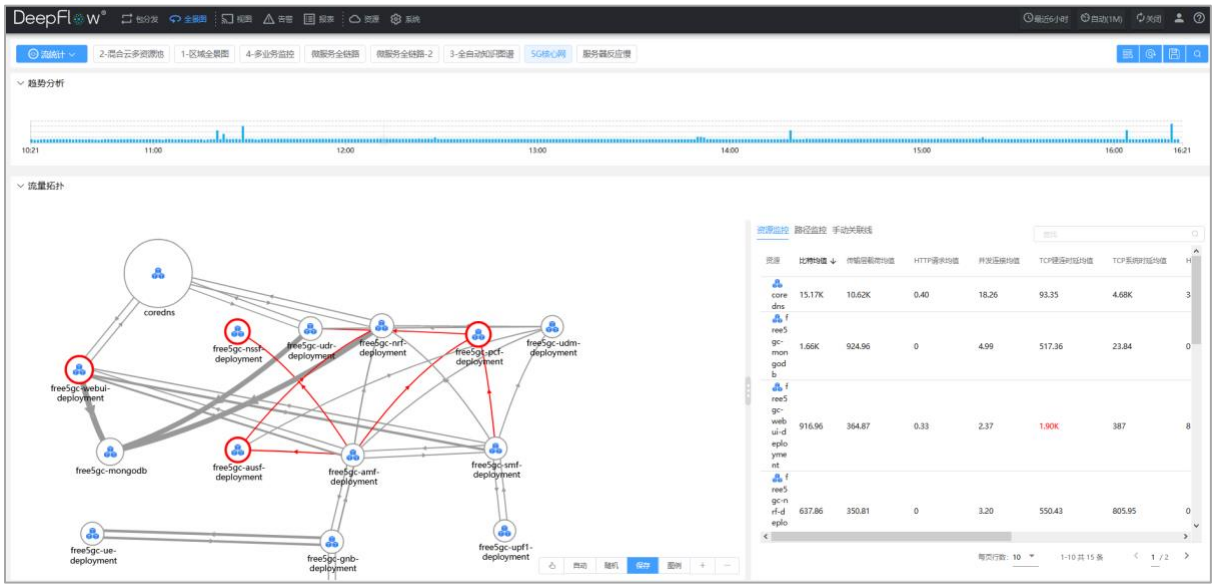
图：Free5GC 界面

在 Free5GC 环境中，DeepFlow®可以快速展示各类型网络功能服务运行及调用全景视图。将服务接口（*SBI，service-based interface*）中的网络各功能间调用通信，以及性能指标进行自动绘制并呈现。



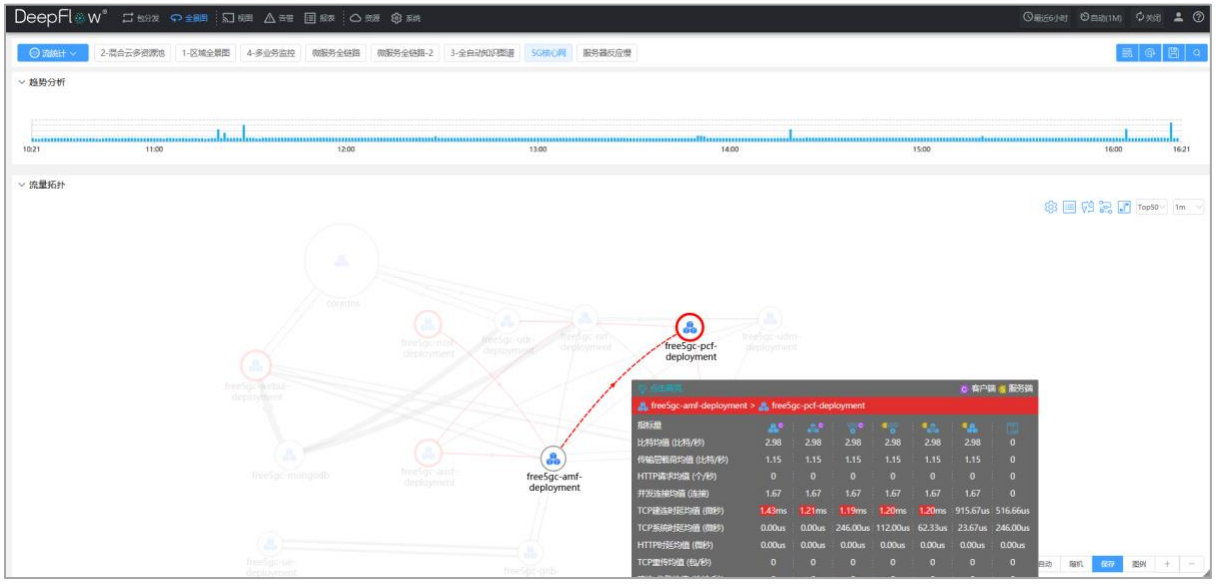
图：功能服务全景图

在实际运行场景，配置 DeepFlow®平台，关注服务间重点指标，包括网络层（*吞吐、载荷*），传输层（*并发连接、TCP 建连时延、TCP 系统时延，TCP 重传、建连失败*）应用层（*Http 请求、Http 时延、Http 异常*），绘制访问调用关系全景视图后，在知识图谱功能支持下，可以迅速关联列举相应的知识维度。



图：全景图性能阈值设置

如果设置指标阈值，比如关注传输层 TCP 建连时延，设置阈值为 1 毫秒，可以及时分析出延时热点。在图示例场景中，可以看到 AMF 网络功能与其他服务间的建连时延较大，并且集中。展开全栈跟踪视图，获取宿主机侧、虚拟机侧以及容器侧的延时瓶颈点。



图：功能服务全栈跟踪

以上 Free5GC 示例运行在实验室环境，模拟运行了相应的测试用例，实际生产场景较实验室更加环境复杂且规模巨大，势必对运维保障提出更高要求。经过实际环境测试验证，DeepFlow®平台也确实能为 5G 核心网填补保障空白。

方案优势

流量采集先进

DeepFlow®5G 核心网监控方案中，主要是以软件采集器实现流量采集，采集器支持 KVM、容器等型号，以进程形态部署安装，最大程度上避免对生产交换平面的干扰，不存在与生产平面交换机流表冲突的风险。虚拟资源具备迁移、回收、重新部署等场景，采集策略跟随保障采集能力在动态环境下的持续一致执行。同时在操作系统上继承进程级隔离保护优势，实现整体系统稳定。

分布式处理系统

优化后的服务间相互调用基于大量东西向流量，对采集到的数据包进行分布式预处理，避免集中单点且资源投入大，写入分布式高新能时序数据库，提升查询展示效率。

场景全规模大

整体方案是基于分布式设计模型以及多地域管理，可以充分保障资源池规模弹性扩展，涵盖虚拟化、容器等多资源池，整体系统可管理 10 万台采集器，满足 5G 核心网服务分拆以及虚拟化后的海量服务规模。

可管理性

平台主控制器是管理员统一集中的采集、分发策略配置、监控诊断交互入口，同时具备对所有采集器状态管理能力。各类分析操作贴近资源池特性，全自动建立知识图谱，梳理多维度信息、指标量，逐级清晰 5G 核心网的复杂环境。

服务全景图

补齐 5G 核心网演进中对虚拟化、容器网络管理短板，关联网络功能，弥补资源池内服务调用监控分析方案，提供运维有效手段，增强对服务化后的基础设施管理能力。

6. 总结

DeepFlow®是一款面向 5G 核心网，应对网络功能服务(NFS)分拆解耦后的新挑战，进行流量采集获取、分发、可视化与监控保障的产品。帮助 5G 核心网在基于服务架构中统一采集服务间的网络流量，实现对访问调用的全面性能监控，并提供容器化后的全栈路径跟踪，补齐 5G 核心网服

务监控空白，应对云原生特点，紧密结合 5G 服务，解决 5G 核心网生产中遇到的监控、运维、保障等难题。本方案已在 5G 核心网环境中验证。

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