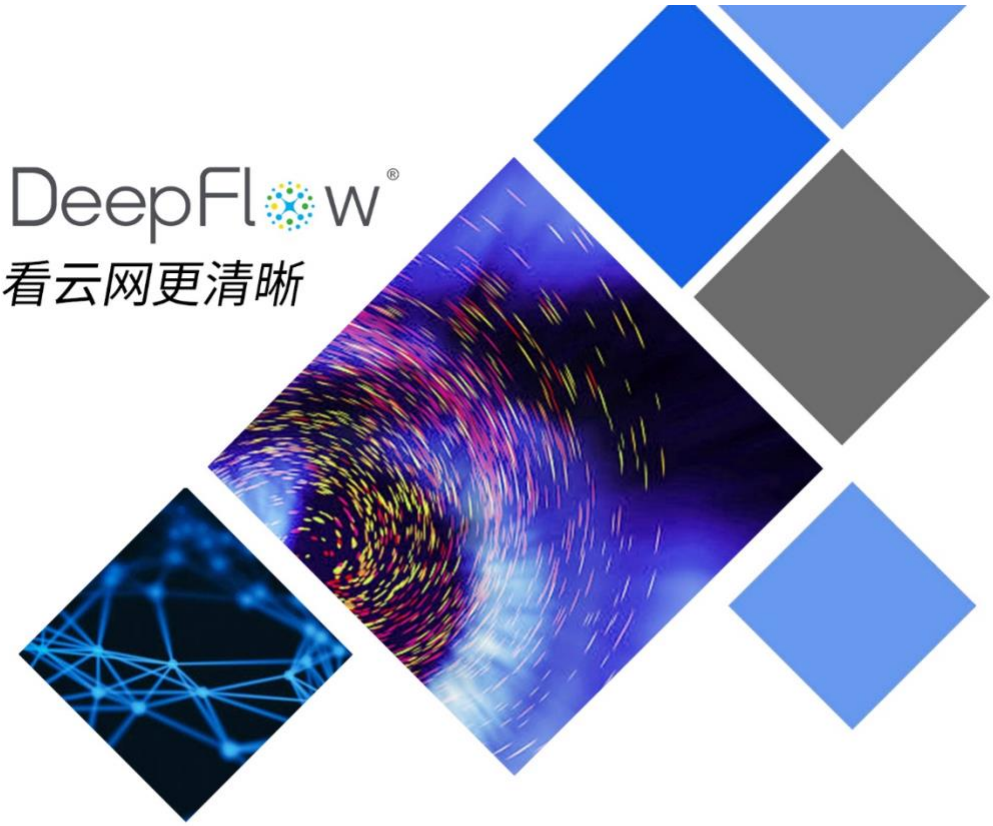
DeepFlow®

看云网更清晰



DeepFlow v5.7用户使用手册

DeepFlow v5.7User Manual

云杉网络

V5.7.2

2021/09/03

目录

1. 总览

总览是面向 DeepFlow 管理员的平台整体状态展现。

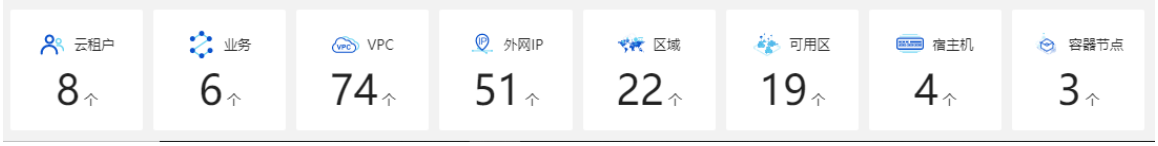
1.1 功能使用

总览页面呈现整个系统运行的概要信息，分为如下图三行。

展现监控网络中采集器、物理采集点、虚拟采集点数量，展现最近一小时采集和分发总流量。

展现最近一个月未结束的告警事件分布、新增的告警事件分布和趋势，及最近 24 小时的最后 5 条告警事件列表。

展现业务层面统计信息包括云租户、业务、VPC、外网 IP 地址数量，以及网络层面统计信息包括区域、可用区、宿主机、容器节点数量。



2. 包分发

通过配置分发策略，用户能精准地将整个虚拟网络以及物理网络中指定流量以最高效的方式分发到多个流量分析工具池（分发点）。

2.1 配置说明

2.1.1 分发策略

一条分发策略由采集点、采集点过滤规则、对端过滤规则、流量处理方法和转发规则五部分组成。

采集点标记流量采集的位置，分为物理采集点和虚拟采集点。采集点过滤可以是指定 VPC 中的一个 IP 地址或 IP 段、一台云服务器、一个子网、一个容器 Deployment 等资源，用户也可通过指定协议和端口号对采集点的流量进行过滤。除此之外，通过指定对端过滤规则，用户也可对采集点过滤的资源的通信对端做精准的限制，实现网络五元组的全方位过滤。

新建/修改说明:

- 采集点过滤规则：计算资源（云服务器）、网络资源（IP 地址、子网）、容器资源（工作负载、容器服务）、业务画像（资源组），上述资源对应的云服务器为实际发生采集分发的点，工作负载则对于实际发生采集分发的 POD。端口号，如果为采集器发送出去的流量则为源端口；如果为采集器接收的流量则为目的端口号。
- 对端过滤规则：从采集点角度来看，采集点之外的都称为对端。比如采集器为云服务器 A，需要统计云服务器 B 与云服务器 A 之间的流量，则云服务器 B 对于采集点云服务器 A 来说就是对端。对端配置端口时，则在采集点上匹配发送出去的流量的目的端口；采集器匹配接收的流量的源端口。
- PayLoad 截断：默认分发的是全包头+全 PayLoad。PayLoad 配置数据则分发的为全包头 + PayLoad 截断的长度。
- 流量标签：对应为 Vxlan 的 VNI、GRE 的 KEY 和 Erspan 的 Session ID。
- 分发策略中：云服务器显示为(名称，别名，区域)，子网显示为(网段，名称，别名

2.1.2 分发点

分发点是接收分发流量的隧道端点，可以是交换机上接收隧道的接口 IP，也可以是具备解析隧道协议的分析工具所在的宿主机/云服务器的接口 IP。

新建/修改说明：

- 隧道类型：目前支持 VXLAN 和 ERSPAN

删除说明：

- 可删除没有分发策略引用的分发点

2.2 配置举例

2.2.1 分发云服务器 vm1 的全部流量

- 采集点过滤规则：云服务器=vm1
- 对端过滤规则：不配置
- 匹配如下流量：
  - vm1 上分发出方向的 src_ip = vm1
  - vm1 上分发入方向的 dst_ip = vm1

2.2.2 发云服务器 VM1 的 tcp 协议的 80 端口的流量

- 采集点过滤规则：云服务器=vm1，协议=tcp，端口=80
- 对端过滤规则：不配置
- 匹配如下流量：
  - vm1 上分发出方向的 src_ip = vm1 and protocol = tcp and src_port = 80
  - vm1 上分发入方向的 dst_ip = vm1 and protocol = tcp and dst_port = 80

2.2.3 分发云服务器 vm1 与云服务器 vm2 之间的流量

- 采集点过滤规则：云服务器=vm1
- 对端过滤规则：云服务器=vm2
- 匹配如下流量：
  - vm1 上分发出方向的 src_ip = vm1 and dst_ip = vm2
  - vm1 上分发入方向的 dst_ip = vm1 and src_ip = vm2

2.2.4 分发云服务器 vm1 与云服务器 vm2 的 tcp 协议的 80 端口通信的流量

- 采集点过滤规则：云服务器=vm1
- 对端过滤规则：云服务器=vm2，协议=tcp，端口=80
- 匹配如下流量：
  - vm1 上分发出方向的 src_ip = vm1 and protocol = tcp and dst_ip = vm2 and dst_port = 80
  - vm1 上分发入方向的 dst_ip = vm1 and protocol = tcp and src_ip = vm2 and src_port = 80

2.2.5 分发 IP 段 192.168.10.24-192.168.10.26 的 80 端口流量

设定 192.168.10.24-192.168.10.30 对应的云服务器为 vm1，vm2，vm3。

- 采集点过滤规则：IP=192.168.10.24-192.168.10.26，端口：80
- 对端过滤规则：不配置
- 匹配如下流量：
  - 分发 vm1 与 vm2、vm3 产生的流量规则如下：

    - vm1 分发出方向的 src_ip = vm1 and src_port = 80 and dst_ip = vm2/vm3
  - 分发 vm1 与 vm2、vm3 以外的流量规则如下：
    - vm1 分发出方向的 src_ip = vm1 and src_port = 80
    - vm1 分发入方向的 dst_ip = vm1 and dst_port = 80

2.2.6 分发子网 192.168.10.0/10 的流量

设定 vm1 为子网 192.168.10.0/10 中的一个云服务器。

- 采集点过滤规则：CIDR=192.168.10.0/10
- 对端过滤规则：不配置
- 匹配如下流量：
  - 分发 vm1 与子网内的云服务器规则如下：
    - vm1 分发出方向的 src_ip = vm1 and dst_ip = 子网内云服务器的 IP
  - 分发 vm1 与子网内云服务器以外的流量规则如下：
    - vm1 分发出方向的 src_ip = vm1
    - vm1 分发入方向的 dst_ip = vm1

2.2.7 分发子网 192.168.10.0/10 与 10.0.0.0/16 子网的 udp 流量

设定 vm1 为子网 192.168.10.0/10 中的一个云服务器。

- 采集点过滤规则：CIDR=192.168.10.0/10
- 对端过滤规则：CIDR=10.0.0.0/16，协议=udp
- 匹配如下流量：
  - vm1 出方向的 src_ip = vm1 and dst_ip = 10.0.0.0/16 子网的 IP and protocol = udp
  - vm1 入方向的 dst_ip = vm1 and src_ip = 10.0.0.0/16 子网的 IP and protocol = udp

2.2.8 分发 vpc1 的全部流量

设定 vm1 为 vpc1 中的一个云服务器。

- 采集点过滤规则：VPC=vpc1，CIDR=0.0.0.0/0
- 对端过滤规则：不配置
- 匹配如下流量：
  - 分发 vm1 与 vpc1 内的云服务器规则如下：
    - vm1 分发出方向的 src_ip = vm1 and dst_ip = vpc1 内的云服务器 IP
  - 分发 vm1 与 vpc1 以外的流量规则如下：

- vm1 分发出方向的 src_ip = vm1
- vm1 分发入方向的 dst_ip = vm1

3. 全景图

全景图是 DeepFlow 两大功能之一，流量监控指标和网络知识图谱全景可视化，通过强大的搜索能力提供云网全景视图下的监控诊断解决方案，结合流日志和 PCAP 数据提供完整的故障回溯取证能力。

3.1 流量搜索

3.1.1 功能简介

全景图流量搜索功能聚焦于从不同的维度对虚拟网络中的流量指标数据进行灵活检索。所有可视化图表（子视图）均可加入视图中进行进一步的组合、设置告警生成策略、设置报表生成策略。

3.1.3 功能使用

3.1.3.1 功能页面

流量搜索从十余个维度的资源视角展示网络性能监控数据。

通过点击拓扑中的节点、路径，以及分布图中的分组，用户可在上述页面之间进行切换，从不同的视角对同样的数据进行展现。另外，上述页面还可进一步跳转到**流量曲线**页面，以折线图的视角，展现现拓扑中的节点、路径或分布图中分组的统计数据在不同时间的结果，并与云服务器、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。进一步的，可以跳转到**流量日志**页面，查看对应的原始流量日志详细信息。

功能使用：
- 时间选择：点击右上角时间控件，可以定位选定时间内的数据展示，开始时间、结束时间支持填写精确时间、相对时间，例如：2021-03-10 15:08:37、now、now/d、now-6d，相对时间支持的时间单位为：s (seconds)，m (minutes)，h (hours)，d (days)，w (weeks)，M (months)，Q (quarters)和 y (years)
- Tip 同步开关：流量搜索、流量曲线增加 Tip 同步开启按钮，实现当鼠标移至某子视图（趋势分析、资源流量排名 Top 折线图、路径流量排名 Top 折线图、流量排名、资源变更事件及所有折线图）后，所有上述子视图 Tip 显示
- 搜索历史-分享：可将设置好的流搜索历史分享给单个账号、管理员账号集合、所有账号集合（单个管理员赋权优先于全部管理员/所有账号赋权），赋予其只读/读写权限，分享来的搜索历史在页面有橘色只读/读写标识
- 禁用/启用：用于临时禁用某个搜索条件

3.1.3.2 流统计

通过输入不同的搜索条件，可实现对统计数据多种维度的过滤、分组、聚合。流量搜索的支持输入多个资源集合，当业务部署在异构资源池中时，可通过多个资源集合的组合将业务呈现在一个视图中。

分组条件：

资源集合中的分组条件描述了统计数据的资源分组标准，由如下条件组成：

- 资源分组
- 采集点分组
- 知识图谱
- 流特征分组
- 流日志特征分组
- HTTP 日志特征分组
- DNS 日志特征分组

资源过滤：

决定如何对监控资源进行过滤，对所有页面均有效，支持从十余个维度对监控资源进行过滤。点击分组、拓扑节点、拓扑路径并进行资源分组的切换操作时，将会自动将该条件设置为选中的资源并重新进行搜索。

其他过滤：

通过指定流量属性过滤条件，可以对匹配的流量做进一步过滤：
- 采集器：支持对流量经过的采集器进行过滤，可用于观测某个采集器上的所有监控数据，经常用于网关虚拟机位置
- 采集点：对流量的采集位置进行过滤，物理网络采集点可在“资源-其他资源-采集点”中进行维护
- IP 类型：
- 监控资源角色：
- 网络协议：
- 服务端口：
- 搜索范围：
- 路径数据：
- 服务过滤：
- 路径统计位置：
- 省份：
- 指标量：

跳转至流量曲线页面后额外支持的过滤条件包括：
- 流量范围：
- 整体：
- 广域网：
- 资源内：
- 资源外：
- 资源间：

路径统计位置：表示流量采集、统计的位置，路径统计数据中支持如下位置（资源统计数据仅支持前两项）：
- 客户端：
- 服务端：
- 客户端容器节点：
- 服务端容器节点：
- 客户端宿主机：
- 服务端宿主机：
- 客户端网关宿主机：
- 服务端网关宿主机：
- 客户端网关：
- 服务端网关：
- 网关：
- 其他：

跳转至流量日志页面后额外支持的过滤条件包括：
- 流日志 - 流量范围：
- 链路协议：
- 应用协议：
- 流日志/HTTP 日志/DNS 日志：
- 客户端口：

- 流日志 ID：

指标量

全景图支持 13 类 122 种指标量，与算子结合可产生 1867 个指标量统计值。除属性类指标量以外均支持 Avg（均值）、Max（峰值）、Min（谷值）、Percentile（百分位数）、Spread（绝对跨度）、RSpread（相对跨度）、StdDev（标准差）七种算子，除时延、负载和属性类指标量以外其他均支持 Sum（总量）算子，属性类指标量支持 Distinct（基数）算子。

子视图

流量搜索通过丰富多样的子视图，对流量数据进行可视化展现。每种子视图均支持一系列标准化操作，其中所有子视图均可支持的操作如下：

- 添加到视图：将子视图添加到选定的视图中，视图中的名称默认复用在全景图中的名称
  - 除了拓扑图以外，添加到视图中的所有子视图均支持生成报表
  - 添加到视图中的所有折线图均支持设置告警
- 下载 CSV 数据：以 CSV 文件的形式下载子视图所使用的流量统计数据，用户可基于 CSV 文件进行二次开发
- 查看 API：查看获取子视图所使用的流量统计数据的 API，用户可通过调用 API 进行二次开发
- 全屏显示：全屏查看子视图，用于对可视区域进行放大，注意放大后子视图部分操作受限
- 弹框显示：弹框查看子视图，对子视图进行放大，且支持对子视图操作
- 切换数据源：除资源变更事件图以外，其他子视图均支持切换数据源，用户也可在系统-数据节点-全景图存储配置中修改和定义数据源
- 修改指标量：修改子视图默认显示的指标量，并设置阈值以便于快速判断指标量与警戒线的关系。不同类型的子视图对该项操作的支持程度存在差别，详见下文介绍
- 样式设置：根据子视图的不同类型，支持对子视图的边距、图例显示、辅助线显示进行设置。

基础拓扑图

未开启链路追踪时，流量拓扑展示为基础拓扑图。基础拓扑图由资源节点及有向路径组成，其资源节点分为两类：

- 监控资源：由搜索条件中分组条件和资源过滤决定的节点
- 表征的资源类型：每个节点表示的资源类型（即图标类型）由搜索条件中的资源分组决定
- 图标外层的圆环：圆环大小表示主指标量统计值的大小，当没有统计值时圆环显示为虚线，当统计值超过阈值时显示为红色
- 节点的悬停操作：展示资源的信息和指标量的统计值，以及分组条件中知识图谱框选择的额外资源属性信息
- 节点的点击操作：点击可查看资源基本信息、资源知识图谱、切换拓扑图展示的资源分组类型、切换至流量曲线页面
- Internet：当监控资源与 Internet 资源存在通信时出现
- 表征的资源类型：表示 DeepFlow 资源-网络资源-子网/IP 页面展示的子网和 IP 之外的 IP 资源

基础拓扑图中的路径表示资源之间的客户端、服务端关系，路径的方向总是从客户端指向服务端：
- 路径的颜色和粗细：路径的粗细表示主指标量统计值的大小，当统计值超过阈值时显示为红色
- 路径的悬停操作：展示两侧节点的关系（客户端->服务端），及在客户端/服务端、客户端/服务端容器节点、客户端/服务端宿主机、客户端/服务端网关宿主机、客户端/服务端网关侧分别采集到的指标量统计值和统计值最大最小的差量。统计位置未显示则可能因为不存在此位置也可能由于未部署采集器导致。统计值的差量可辅助判断路径上产生的网络丢包和时延。
- 路径的点击操作：与节点的点击弹出页相似

基础拓扑图支持如下标准化操作：
- 基础操作
  - 添加到视图
  - 下载 CSV 数据
  - 查看 API
  - 全屏显示
  - 弹框显示
  - 切换数据源
  - 修改指标量
- 其他操作
  - 切换 Top：通过选择 Top 20 下拉框，可调整拓扑图中显示的监控资源点数量
  - 最多展示每个资源集合内 Top N 个携带指标数据的资源（实圈）
  - 由拓扑路径关联展示的、不在上述 Top N 中的资源不会携带指标数据（虚圈）
  - 当上述 Top N 资源没有关联任何 Top N 路径时，会从最终拓扑图中消除
  - 每个资源集合中的上述 Top N 资源，分别展示它们访问 Internet、本资源集合内部、其他每个资源集合的 Top N 路径
  - 每个资源集合中的上述 Top N 资源，分别展示 Internet、本资源集合内部、其他每个资源集合访问他们的 Top N 路径
  - 展开表格：点击后展开所有资源和路径数据的统计表格，支持搜索、排序、过滤操作，点击表格的一行左侧拓扑图可同步高亮，再次点击表格一行可弹出资源信息显示页；点击左侧拓扑图中的资源或链路项，表格中相关资源与链路联动高亮
  - 名称缺省显示/名称全称显示：点击后在全名和名称前缀之间切换，避免名称太长造成遮挡
  - 开启链路追踪/关闭链路追踪：点击后切换基础拓扑图与全链路拓扑图 - 颜色设置：点击后可自定义基础拓扑图的圈/线颜色
  - 补齐所有关联数据：默认状态下不做补齐，排名未进入 Top N 的数据无法展示，例如 Top N 的点可能缺少部分采集点的数据（选择按采集点分组时），Top N 的路径可能缺少部分统计位置或采集点的数据
  - 显示资源逻辑关联：点击后根据负载均衡器规则、NAT 网关规则、资源组依赖关系自动补充负载均衡器与后端云服务器/IP、NAT 网关与 NAT 后的云服务器/IP、

资源组之间的逻辑线，当存在流量线时则不补充逻辑线
- 显示特征关联关系：点击后补齐流/包特征节点与资源节点的连线
- 拓扑位置操作 - 放大缩小
- 保存：记忆节点位置，需要用户先保存搜索条件
- 随机：随机排布拓扑中的节点
- 自动：智能排布拓扑中的节点
- 图例：拓扑图图标说明，以及圆圈大小、线条粗细说明
- 手动补充资源关系模式：点击后进入手动补线模式，通过点击拓扑图上两个节点，则补充一条线，再次点击后回到拓扑图展示

知识图谱

点击资源或路径弹出框时，点击知识图谱，则将根据资源或路径的关联信息绘制星状的拓扑图
- 拓扑操作
  - 点或者路径的悬浮：高亮关联的点与路径，并展示点的全名
  - 点点击：将绘制当前点对应资源的知识图谱
  - 其他操作：支持拓扑图放大缩小，查看图例 - 拓扑逻辑：
  - 同类型的点，最多只展示 2 个，其他统一收入到$num 个资源类型，比如 100 个虚拟机

非对称拓扑图

当高级搜索分组条件选择了流特征分组或包特征分组时，拓扑图将展示为非对称形式。具体来讲，图中每条路径有两种情况：
- 资源 A -> 资源 B+特征分组信息：A 作为客户端访问 B，并携带该特征分组信息
- 资源 B+特征分组信息 -> 资源 B：为了将资源 B 的各种特征分组信息节点汇集起来显示的虚拟路径，无统计数据。但是若资源 B 在整个拓扑中只有一个特征分组信息，则会自动隐藏这条连线（即将上述两个资源节点合并为一个节点）。

非对称拓扑图支持的标准操作与基础拓扑图相同。

3.1.3.3 链路追踪

全链路拓扑图

当开启链路追踪时，流量拓扑展示为全链路拓扑图。其下半部分为基础拓扑图，点击其中的节点和路径可在上半部分显示对应的虚拟和物理链路：|
- 物理链路：
  - 采集点分组=是，可查看物理链路，当基础拓扑图路径对应的流量的采集点为非虚拟网络时，则高亮对应的链路
  - 路径的颜色和粗细：路径的粗细表示主指标量统计值的大小，当统计值超过阈

值时显示为红色，否则显示为绿色
- 路径的悬停操作：展示两侧的物理网元，及在两个采集点分别采集到的指标量统计值。若两侧均有统计值，二者的偏差程度可辅助判断链路上的丢包和时延。
- 路径的点击操作：点击可查看物理网元的基本信息、切换至流量曲线页面查看与之关联的流量拓扑中资源间流量的历史统计值
- 点的颜色和粗细：点的粗细表示点连接的所有路径上主指标统计值的最大差量大小，可辅助判断网元上的丢包和时延。
- 点的悬停操作：展示网元的信息和相邻路径上的最大指标量差值
- 虚拟链路：基础拓扑图路径对应的虚拟网络流量统计位置
- 采集点分组=是，且存在虚拟网络采集点流量时，展示路径对应的虚拟链路
- 路径的悬停操作：展示两侧的统计位置的基础拓扑图路径指标量统计值。若两侧均有统计值，二者的偏差程度可辅助判断链路上的丢包和时延。
- 路径点击操作：弹出链路追踪详情图
- 点的悬停操作：展示当前统计位置的基础拓扑图路径指标量统计值
- 点点击操作：弹出链路追踪详情图

全链路拓扑图支持的标准操作相比基础拓扑图，加入：
- 拓扑位置操作
- 分割线调整：物理拓扑图与基础拓扑图的分割线上下可调

链路追踪详情图

当点击全链路拓扑图的虚拟链路时，弹出链路追踪详情图，展示虚拟链路各个统计位置对应的资源、采集点、采集网卡标识、指标量数据等信息
- 虚拟链路点击点或者路径时，可高亮链路详情表的对应的行
- 点击链路详情表的行，可出现弹出框，支持跳转到流量曲线和流量日志页面

链路追踪详情图支持的标准操作包括：
- 基础操作
- 下载 CSV 数据
- 查看 API
- 切换数据源
- 修改指标量：可选择指标量
- 切换显示指标量：按选中的指标量显示链路柱状图

3.1.3.4 流量日志

从流量曲线可跳转至流量日志页面，查看对应的流量日志详情，提供回溯取证的能力。

异常提示：
- 某区域内的数据查询不全时，流量日志页面子视图趋势图、表格出现异常提示查询数据异常

- 当整个区域内的数据查询都失败时，区域 tab 页右侧提示用户查询数据异常异常区域：$区域名称

流日志

流日志数据是基于五元组聚合存储的流数据，对于五元组对应的连接超过 1 分钟的情况会每隔 1 分钟输出一次当前流的信息。

相比指标数据，流日志能提供的额外能力为：
- 查看每条流的详细属性和指标量统计值，总共支持查看近 100 个参数 - 查看每条流的源端口号 - 查看每条流的双端 MAC 地址、链路协议、VLAN
- 查看每条流的隧道类型、隧道 ID、双端隧道 IP
- 查看每条刘的双端真实 IP，即使是 Internet 上的 IP（在指标数据中记录为 0.0.0.0），流日志中也会进行记录
- 查看每条流的应用协议，包括 HTTP、DNS 和其他

HTTP 日志

HTTP 日志是基于客户端与服务端之间的 HTTP 流量提供的日志，可查看 HTTP 流量中报文类型、协议版本、请求方法、代理客户端、响应码以及请求与响应包时延等信息

DNS 日志

DNS 日志是基于客户端与服务端之间的 DNS 流量提供的日志，可查看 DNS 流量中报文类型、查询域名、解析地址、响应码以及请求与响应包时延等信息

3.2 流量下载

3.2.1 流量下载

通过点击全景图的流量下载，可创建、查看以及修改 PCAP 策略，PCAP 策略能针对虚拟网络以及接入网络的计算资源（云服务器）、网络资源（IP 地址、子网）、容器资源（工作负载、容器服务）、业务画像（资源组）等维度生成的 PCAP 文件，也能进行 ACL 策略的过滤，让用户更关注于所需报文：
- PCAP 策略的后端匹配规则与分发策略的后端匹配规则一样，可参考分发功能 - 可根据流量来源来确定需要进行 PCAP 文件保存的对象是虚拟网络还是接入网络的镜像口
- PCAP 策略的 PayLoad 截断，可设置，默认为 0，即表示截断为 0，只截取包头
- 采集点选择虚拟网络时，截断长度支持 0-65535 的整数，当输入值大于 1000 时，需将采集器 PCAP 套接字配置为 TCP，否则实际生效值仅为 1000
- 采集点选择物理网络时，截断长度支持 0-65535 的整数
- 名称点击时可查看 PCAP 策略生成的文件的个数和大小曲线详情图
- PCAP 策略生成的文件是按照后端配置文件设置的最大超时时间与最大切割文件大小共同生效的，默认超时时间为 5min，切割文件大小为 25M

- PCAP 文件个数：此策略当前系统中存在的 PCAP 文件的个数，包含最新的用户不可见的 tmp 文件
- PCAP 文件大小：此策略当前系统中存在的 PCAP 文件大小的总和，包含最新的用户不可见的 tmp 文件

通过页面点击 PCAP 策略的查看详情按钮，可选择任意时间范围内的生成的 PCAP 文件，并对需要下载的 PCAP 文件进行选择，然后点击直接下载或者间接下载：
- 采集器名称：对应生成 PCAP 文件的采集器名称
- 采集网口识别：对应采集器的采集网口的 MAC 地址
- 直接下载：直接将选择的 PCAP 文件进行合并下载
- 过滤下载：用户可对选中的文件按 IP 类型，协议，端口以及 IP 进行筛选下载。
- 过滤下载端口：是指 PCAP 文件的匹配的任意源端口或者目的端口
- 过滤下载 IP:是指 PCAP 文件的匹配的任意源 IP 或者目的 IP

3.3 网络拓扑

全景图网络拓扑功能聚焦于从逻辑、虚拟、物理的视角展现网络的配置和状态指标数据。

3.3.1 逻辑拓扑

3.3.1.1 租户视角

通过指定输入需要查询的信息，可从 VPC，子网，安全组，云服务器，IP 的角度查看的资源层级以及连通性关系，通过悬浮、展开收起等功能可查看流量大小、云平台以及资源统计量等信息。通过添加查询条件到常用，可保持为常用按钮，更快速点击查看。

说明：
- 默认显示：如果添加常用按钮时，按照常用的第一个显示；如果未添加常用按钮，则不显示页面。
- 云服务器节点：云服务器属于多个子网时，会在每个子网都复制一个云服务器节点
- 路由节点：只支持 openstack，公有云，可支持查看路由表
- 安全组节点：支持 openstack，公有云，可悬浮查看安全组规则。每个云服务器如果关联安全组都复制一个安全组节点，没有挂任何云服务器的安全组不会出现在拓扑界面。
- 悬浮：查看节点资源管理信息和流量大小，蓝色链接点跳转到资源管理和流量统计

3.3.1.2 管理员视角

通过指定类型为宿主机，宿主机下拉框可查看具体宿主机的资源层级以及连通性关系，通过悬浮、展开收起等功能可查看流量大小、云平台以及资源统计量等信息。通过添加常用宿主机，可快速查看和点击经常使用的宿主机的资源拓扑。

说明：根据当前宿主机上的云服务器所属的 VPC 统计，宿主机的拓扑也是根据云服务器所属的 VPC，路由器，子网，安全组等关系展开。

3.3.2 连通性诊断

通过输入 IP，协议加端口这些查询条件，可查看 IP 的逻辑网络关系以及虚拟网络组网情况，帮助用户从逻辑网络配置层面检查连通性：
- 对云服务器状态、安全组规则、对等连接和路由器表项进行判断并检测是否影响网络连通性
- 支持两端都为内网 IP 或者外网 IP 进行检测
- 安全组检测：检测时会根据安全组的优先级，以及安全组规则的优先级来进行匹配，如果安全组的允许规则被匹配则认为检测通过；如果安全组的拒绝规则被匹配或者未匹配任何安全组规则则认为检测不通过。
- 路由器表项检测：只在不同 VPC 的两个云服务器通信检测，如果 VPC 直接建立了连接则判断路由规则是否放通连接。

4. 视图

视图是用户自定义监控图表的窗口。目前用户可将全景图-流量搜索中的任意图表加入视图中，并对其中的任意折线图设置告警策略，以及对整个视图设置报表生成策略。同时可以将视图自由分享给不同账户。

4.1 功能介绍

视图页面提供用户自定义功能可视化的能力，可将 DF 中各功能图表自由组合，并提供告警(针对时间维度呈现图表)和报表能力。

视图由子视图组成，每个子视图是一个独立的可视化功能模块，可以通过子视图的布局调整工具来灵活调整子视图的大小和位置。

视图可以加入全景图中的所有图表。

视图中每个子视图(图表)提供了一组标准化的图表操作，包含功能页中的所有操作。此外，子视图独有的操作包括：

- 告警

  时间维度折线图可打开告警配置界面。在该界面中，可以

  - 管理告警策略
  - 开启禁用告警策略
  - 开启禁用折线图中加载告警策略的告警事件段
  - 查看告警策略对应的告警事件
- 打开原功能页面

  子视图会记录加入视图时的查询过滤条件，可以通过打开原功能页面按钮返回对应的功能页面，并加载加入时的查询条件。

视图层面，支持功能包括

- 创建报表策略

  对当前视图创建报表策略，定时生成可下载的离线报表。

- 全屏

  将视图的内容全屏展示，适合在大屏场景下演示。

- 显示模式切换

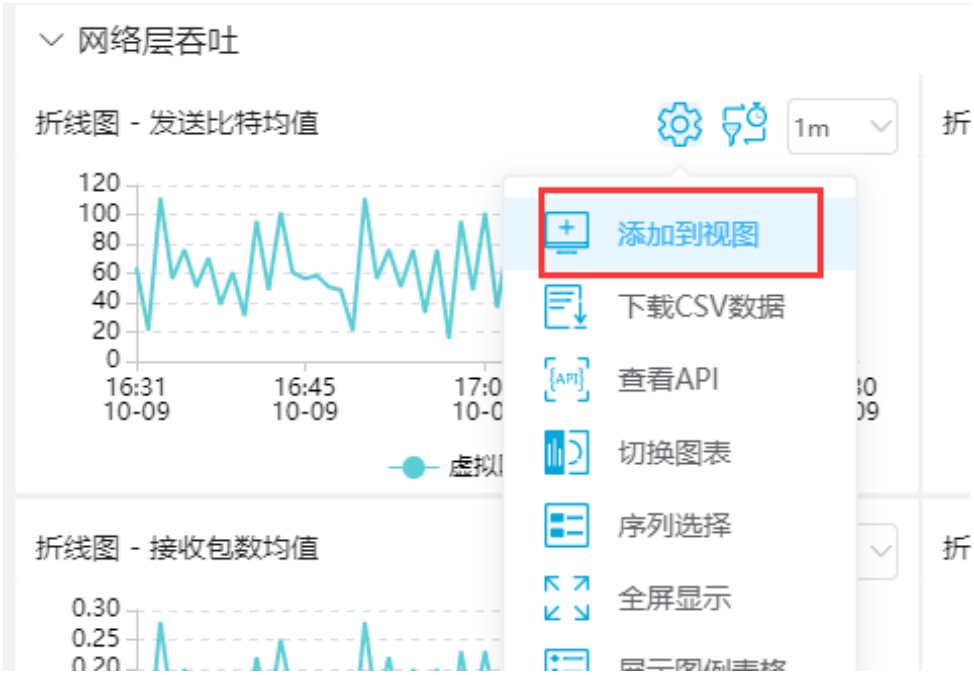
  可切换至深色模式，满足大屏演示需要。

- Tip 同步

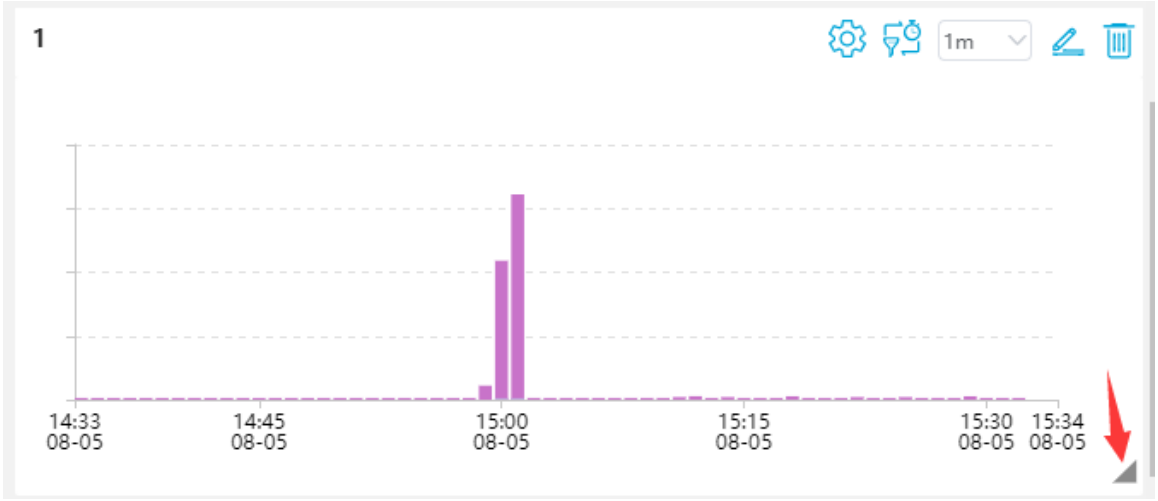
  可切换趋势类子视图所有 Tip 同步显示或只显示鼠标所指子视图

4.2 功能使用

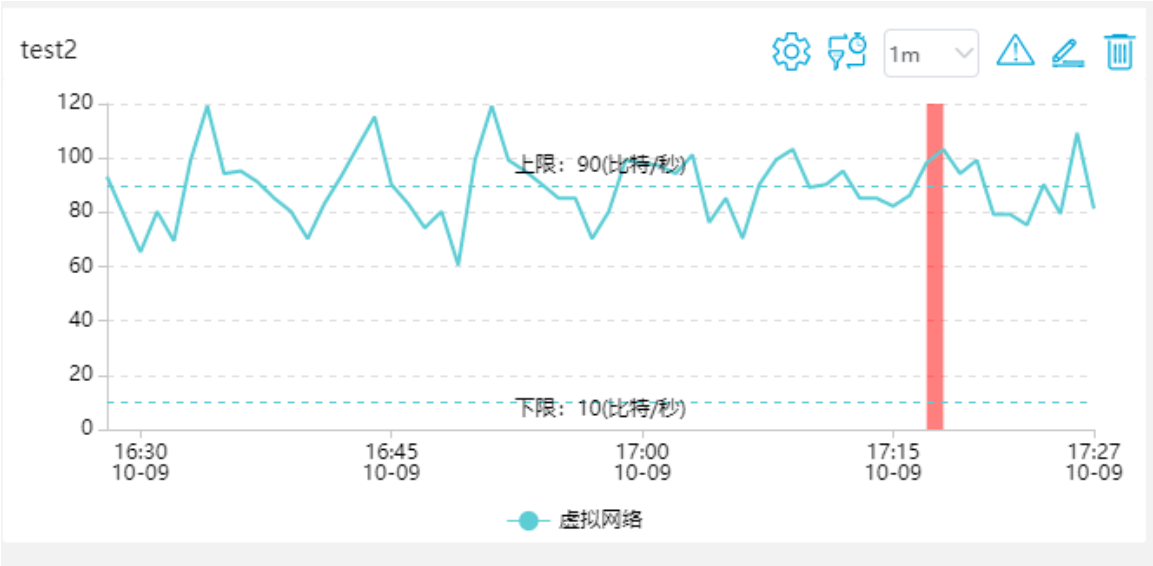
- 全景图功能页中选择任意子视图，点击添加到视图按钮并保存

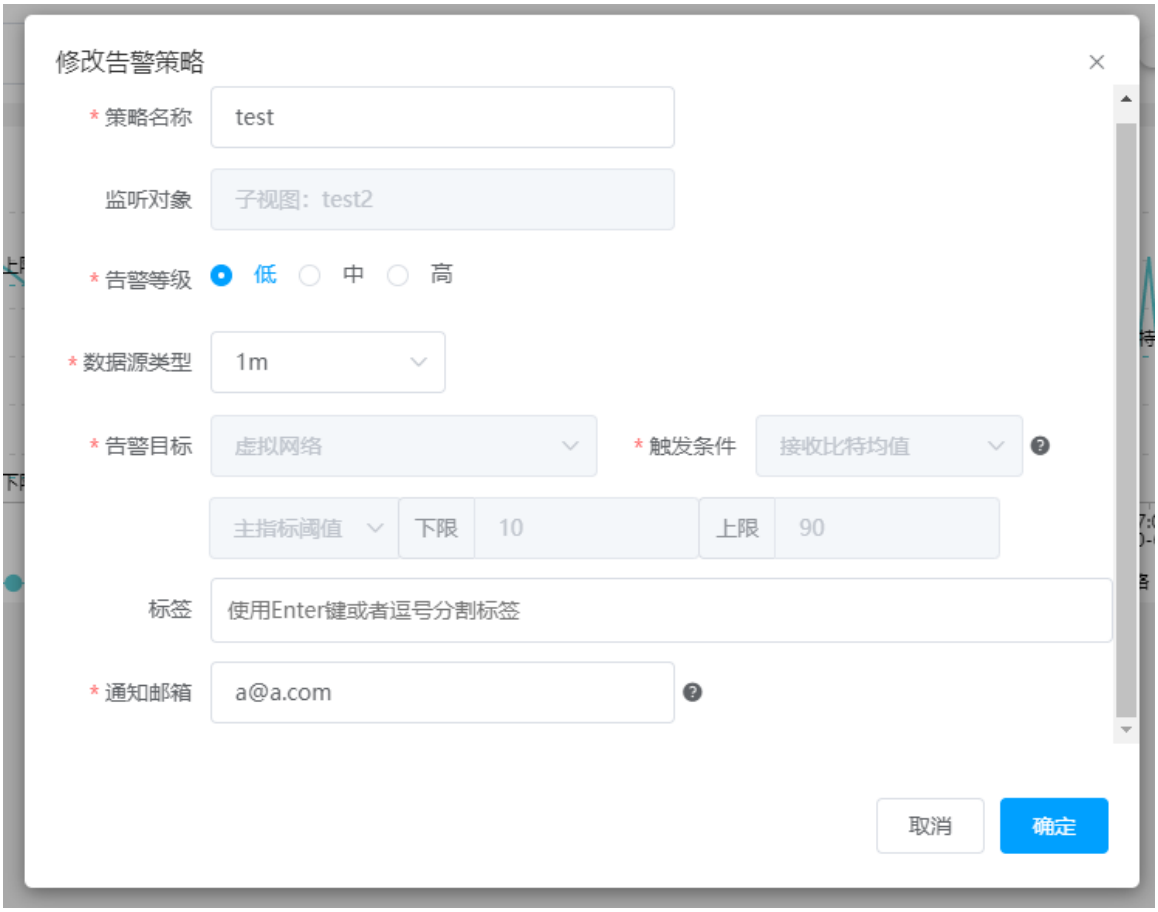


- 通过子视图的右下角调整大小，也可在标题处拖动子视图，调整视图的布局。



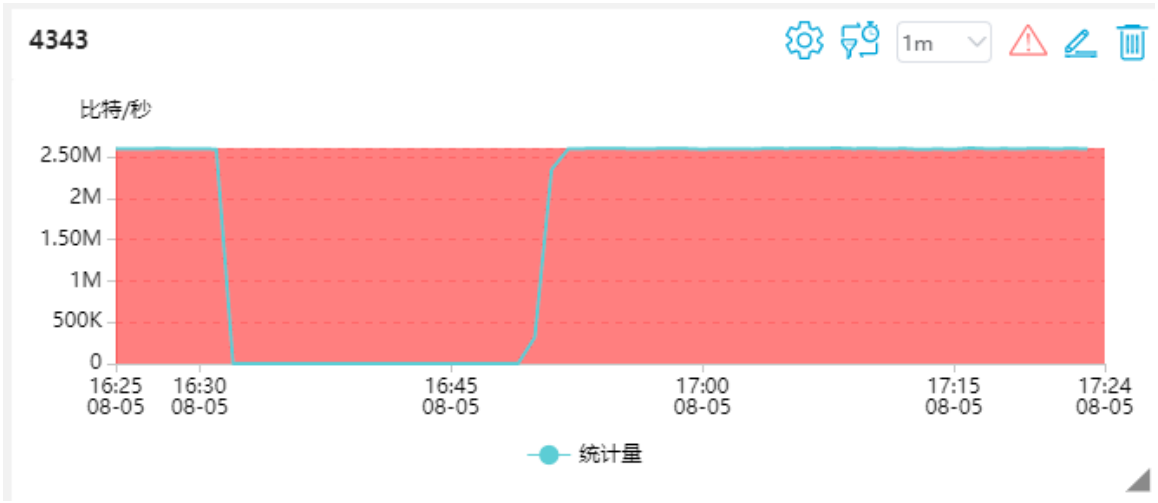
- 为流量设置告警策略





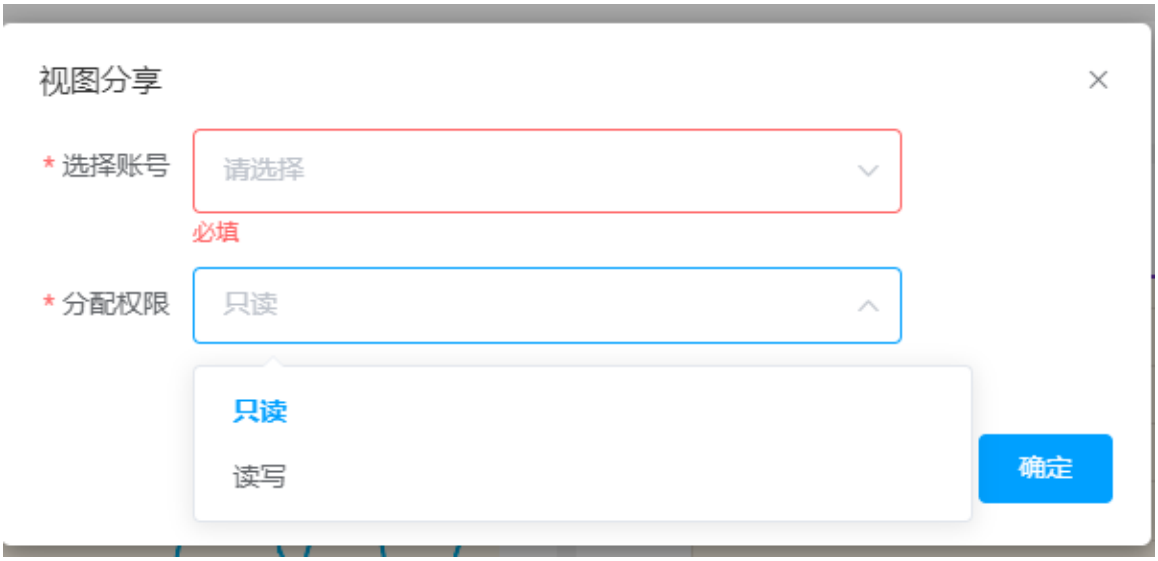
- 对创建成功的告警策略可以启用禁用，或者进行修改、删除

- 默认状态下，折线图会自动加载对应的告警事件时间段，以红色背景显示



- 可以在视图右上角为视图创建报表策略

- 可在视图右上角分享该视图分享给单个账号、管理员账号集合、所有账号集合（单个管理员赋权优先于全部管理员/所有账号赋权），赋予其只读/读写权限，分享来的视图在页面有橘色只读/读写标识



注意：当租户与管理员间有共享的视图时，管理员需要将创建此视图的租户账号锁定，才可修改此视图

- 视图支持导出为模板文件，并可导入对应的模板文件生成新的视图
- 视图支持添加模板变量，被每一个子视图引用，通过模板变量切换控制子视图的搜索条件
- 支持子视图划分模块管理，按照用户需求归类查看子视图

5. 告警

告警策略包括阈值告警和系统告警两种。其中阈值告警在子视图中创建；系统告警由系统自动创建，暂不支持手动管理。

5.1 功能介绍

5.1.1 告警策略

集中管理平台所有 APP 的告警策略。APP 负责告警策略的创建，创建好的策略，将统一在此处纳管。用户在该功能页查可查看到所有的告警策略，包括设定的平台自身的系统告警策略。告警策略中支持固定阈值进行触发。

告警策略包括阈值告警和系统告警两种。其中阈值告警在子视图中创建；系统告警由系统自动创建，暂不支持手动管理。

5.1.2 告警事件

告警策略定义的规则从指定的数据源中监控到的异常，并按照规则聚合成告警事件，并推送给用户。

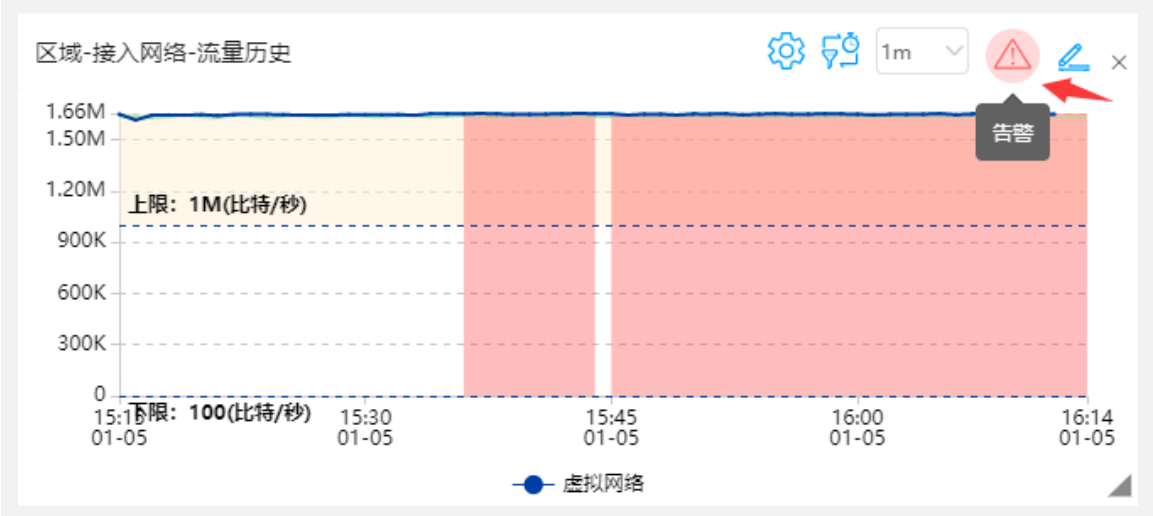
5.1.3 推送端点

告警支持配置多种推送规则，邮件推送、HTTP 推送、PCAP 策略开启/关闭

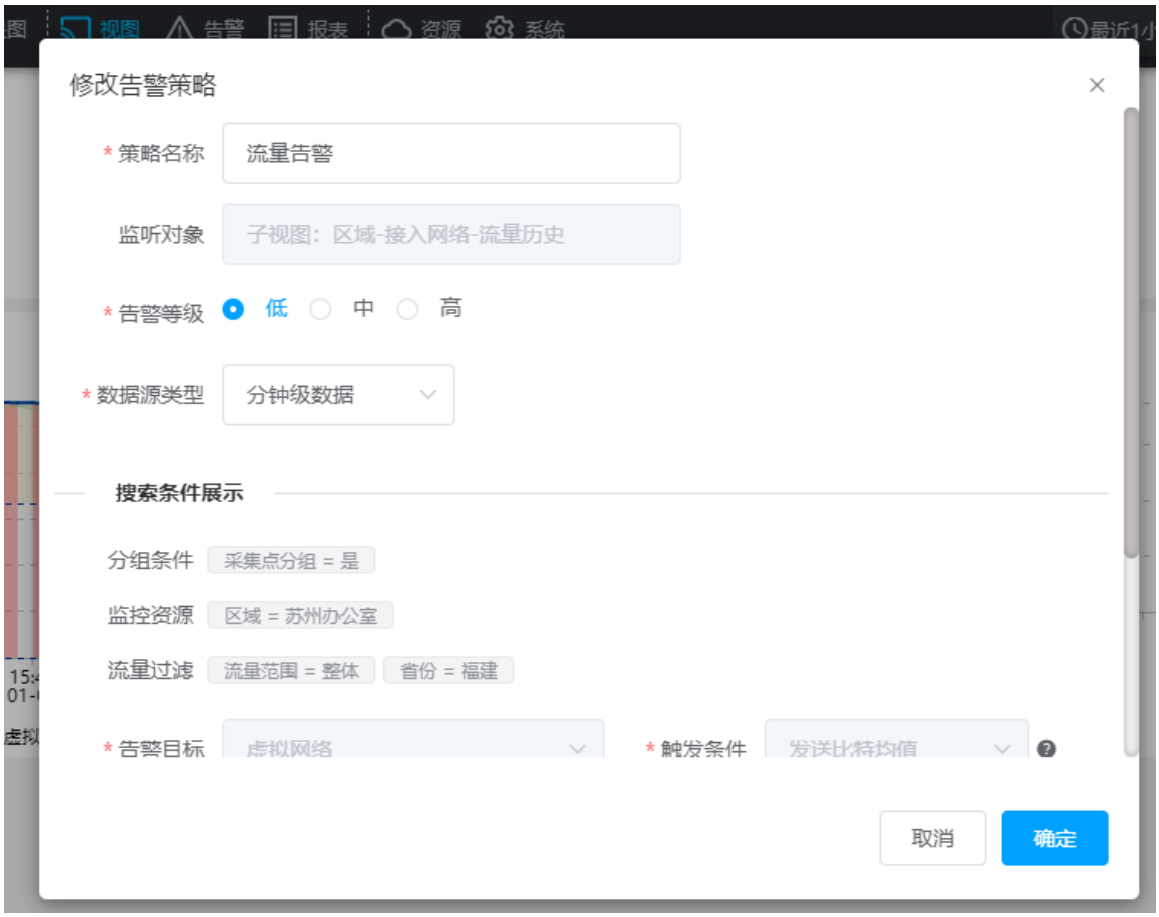
5.2 功能使用

5.2.1 创建告警策略

子视图中可以创建阈值告警。目前支持时间维度的折线图，以及 TopN 折线图。其中，TopN 折线图告警对超出上限的每条线进行告警。

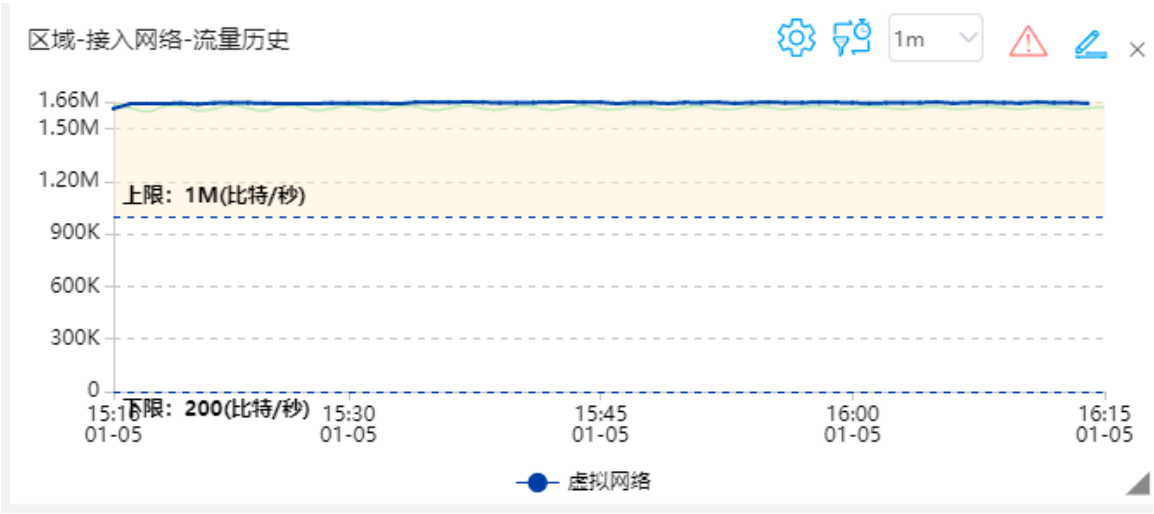


其中，各项配置为：
* 策略名称，用于标识告警策略的名称
* 监听对象，固定为子视图，不可修改
* 告警等级，标识告警策略的严重程度
* 数据源类型，选择所读取的数据源类型。注意此处选择和子视图独立，互不影响。
* 搜索条件展示，不可修改，为创建告警策略时绑定的查询条件。后续子视图修改不会影响告警策略的搜索条件。
* 告警目标，固定为子视图的统计量
* 触发条件，固定为子视图的主指标量
* 上下限，在选择的指标量超出上限或低于下限时触发告警策略，上下限自动从主指标阈值同步（TopN 折线图只支持上限）
* 标签，用于给告警策略添加文字标签
* 通知邮箱，用于发送告警时间的邮箱地址，支持最多 10 个

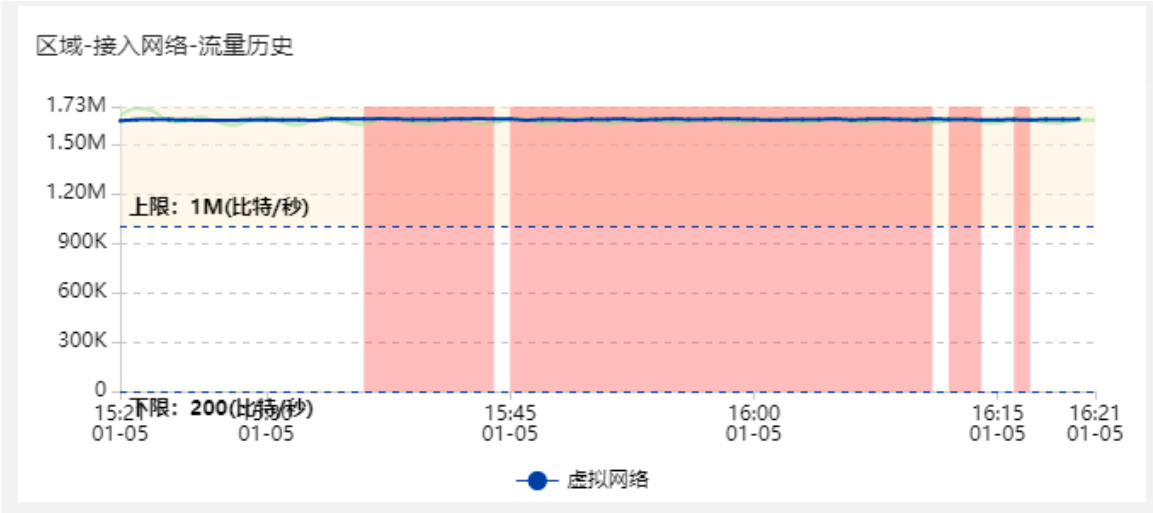


5.2.2 子视图加载告警事件时间段

- 发生告警时，会在告警事件发生和结束时通过告警策略配置的邮件发送告警通知。
- 子视图的告警图标在数据范围内，会显示为红色



- 开启展示告警后，会显示时间段内的告警事件



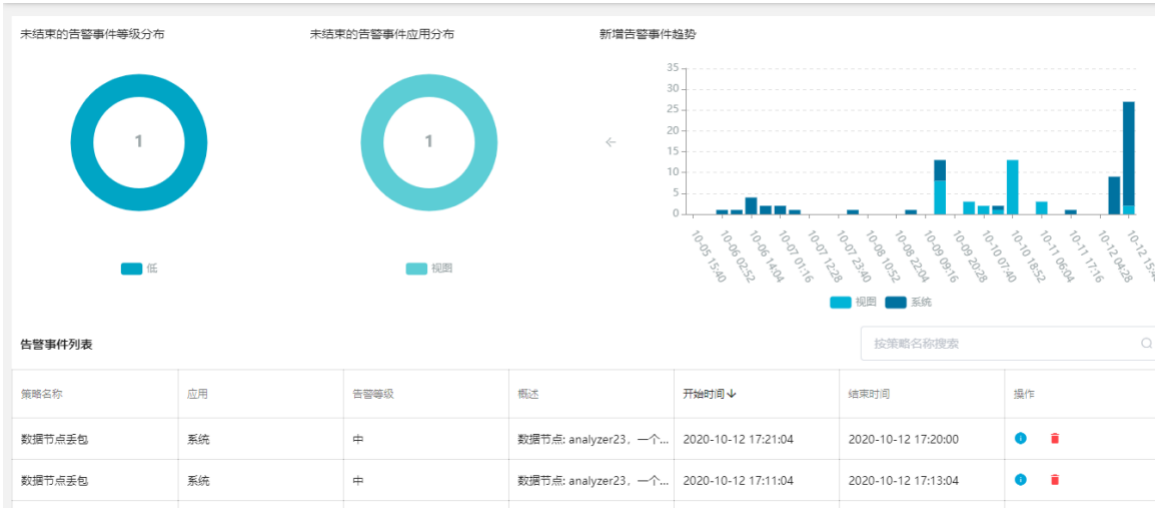
5.2.3 告警策略列表

- 告警策略列表集中呈现系统告警策略与视图告警策略，并可设置告警策略状态、编辑、删除告警策略（系统告警策略不可删除），并可呈现告警策略的触发条件

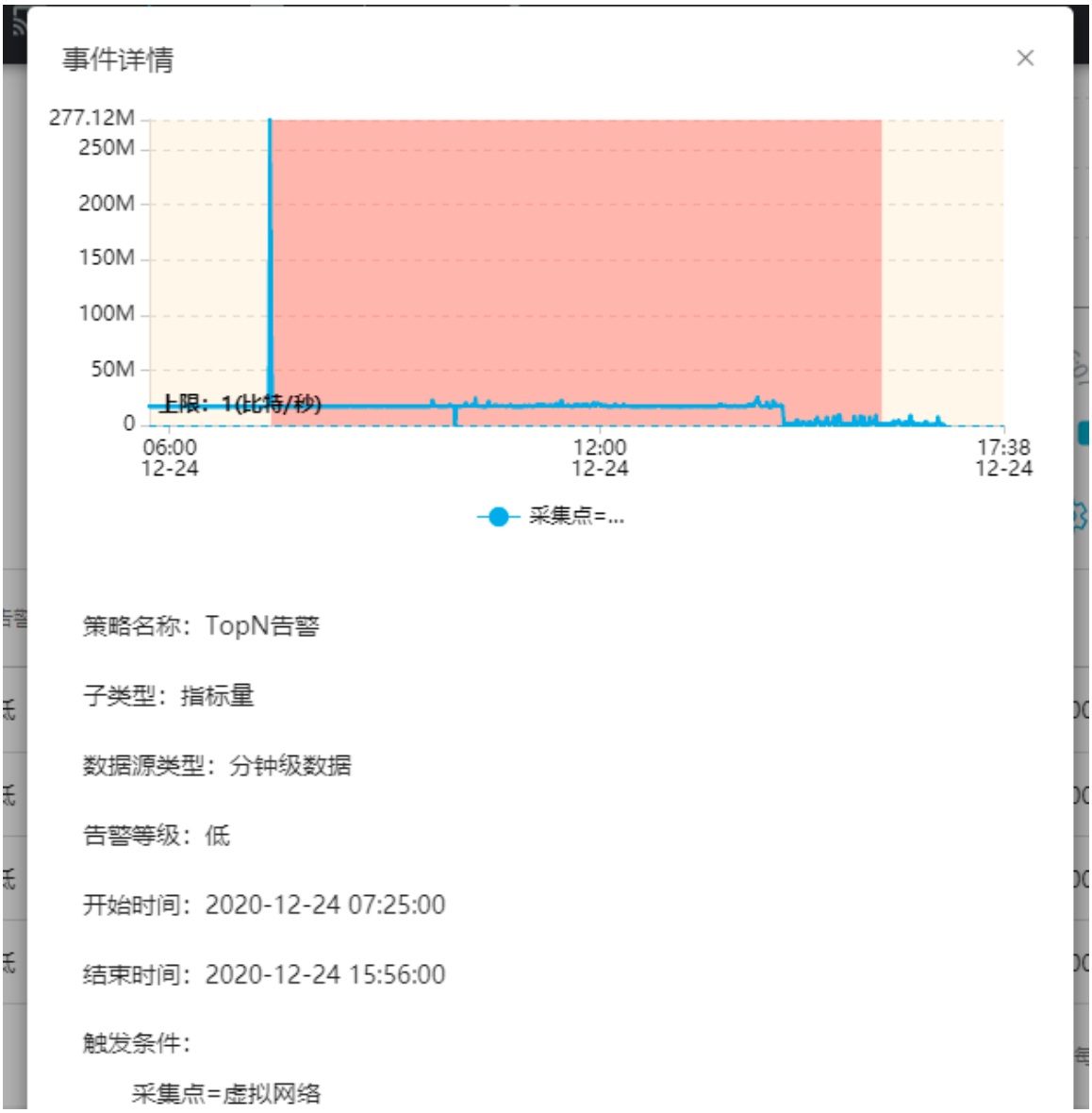
- 点击单个告警策略对应的事件数量后，跳转至告警事件列表页对该策略的过滤结果

5.2.4 告警事件列表

- 告警事件列表包括未结束的告警事件统计，新增告警事件统计和告警事件列表



- 告警事件可点击查看详情，其中阈值告警可以返回到对应的子视图对应的告警时间段，并显示对应时间段的流量情况。



5.2.5 推送端点

- 配置推送端点时，启用策略开启表示告警事件开启时推送，禁用策略开启表示告警事件结束时推送
- 目前支持配置 Email 推送、HTTP 推送、PCAP 推送

6. 报表

通过视图创建报表，每日推送对应的报表结果。

6.1 功能介绍

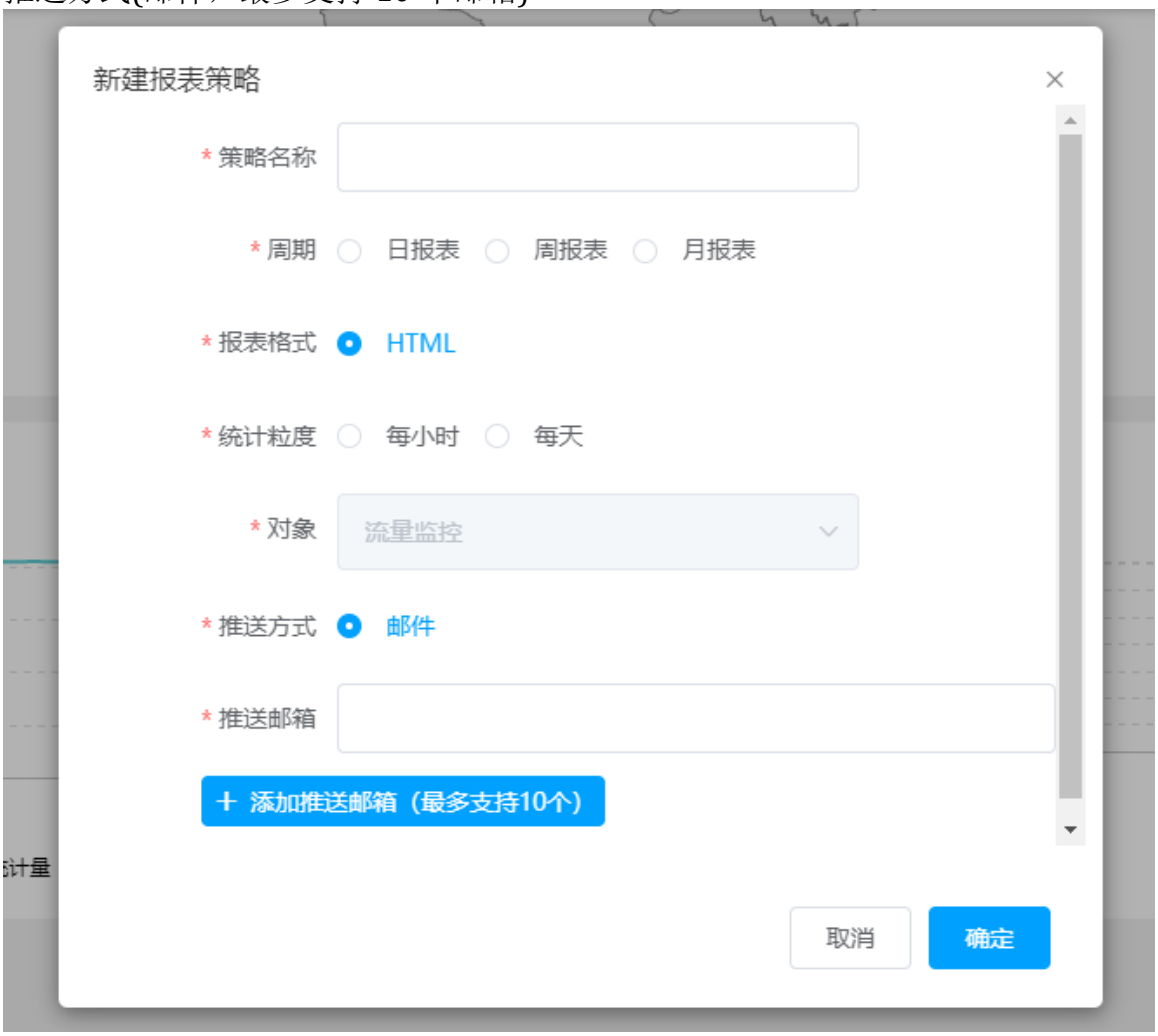
视图中可以创建报表，定时推送给用户，以离线下载 html 的格式，记录报表周期内的视图结果。

6.2 功能使用

- 视图中创建报表

  其中可设置

  - 策略名称
  - 周期
  - 统计粒度
  - 对象(固定为当前视图)
  - 推送方式(邮件，最多支持 10 个邮箱)



建议： 报表的生成策略为每日推送。例如周报表，每天推送上一周(如 上周二-这周二)的报表。报表从起点时间的当天 0 点，到结束时间的当天 24 点。每次报表策略的修改，以生成报表前的最后一次为准，并从当天开始影响后续生成的报表，对之前的报表不会有影响。

- 查看报表策略列表

  在报表-策略中查看所有的报表策略列表

  点击策略名称，可以跳转到报表列表页查看对该策略的过滤结果。

- 查看报表列表

  在报表-列表中查看所有生成的报表结果，按生成时间逆序排列(最近生成的在最前)。可以下载离线 html 包，或者删除无用的报表。报表中子视图支持下载 CSV 数据。

7. 资源

7.1 资源管理

自动或手动同步云网中的资源信息，是全景图十余个维度搜索能力的基石。

7.1.1 功能使用

7.1.1.1 概念映射

资源管理将不同厂商的云平台进行抽象和整理，适配统一的概念，DeepFlow 平台的其他应用都基于统一的概念来分析和呈现数据。

7.1.1.2 页面操作

所有表格信息均支持 CSV 下载与列选择，部分资源信息支持设置别名。

- 资源池
  - 支持录入区域，支持修改区域的经纬度，用于在全景图中绘制正确的区域地图
  - 支持录入可用区，支持在录入可用区时与区域关联
  - 支持录入云平台，用于资源对接；支持修改云平台配置
- 计算资源
  - 支持录入云服务器与网卡，支持指定区域、可用区、云平台、VPC、类型、宿主机
  - 支持录入宿主机与网卡，支持指定区域、可用区、云平台、管理 IP、类型
  - 点击云服务器名，可查看云服务器虚接口的采集和分发速率
- 网络资源
  - 支持录入 VPC，支持将录入的 VPC 与区域关联
  - 支持录入子网，支持将录入的子网与区域、可用区、VPC 关联
  - 对于录入的子网，支持指定子网的类型（外网/内网）和网段（多个 IPv4/IPv6 CIDR）
  - 支持查看路由器的路由表
- 网络服务
  - 支持查看安全组、NAT 网关、负载均衡器的策略表
- 容器资源
  - 支持查看服务、Ingress 的策略表
- 其他资源
  - 支持录入物理网元并指定其类型和区域
  - 支持录入物理采集点，采集点支持镜像、分光、sFlow、NetFlow
  - 支持录入物理链路，关联两侧的物理网元和采集点
  - 支持录入资源组、云平台的自定义图标

7.2 业务画像

业务画像可将 VPC 或者子网的资源通过流量进行梳理，得到这组资源内部的应用服务依赖和流量访问关系。

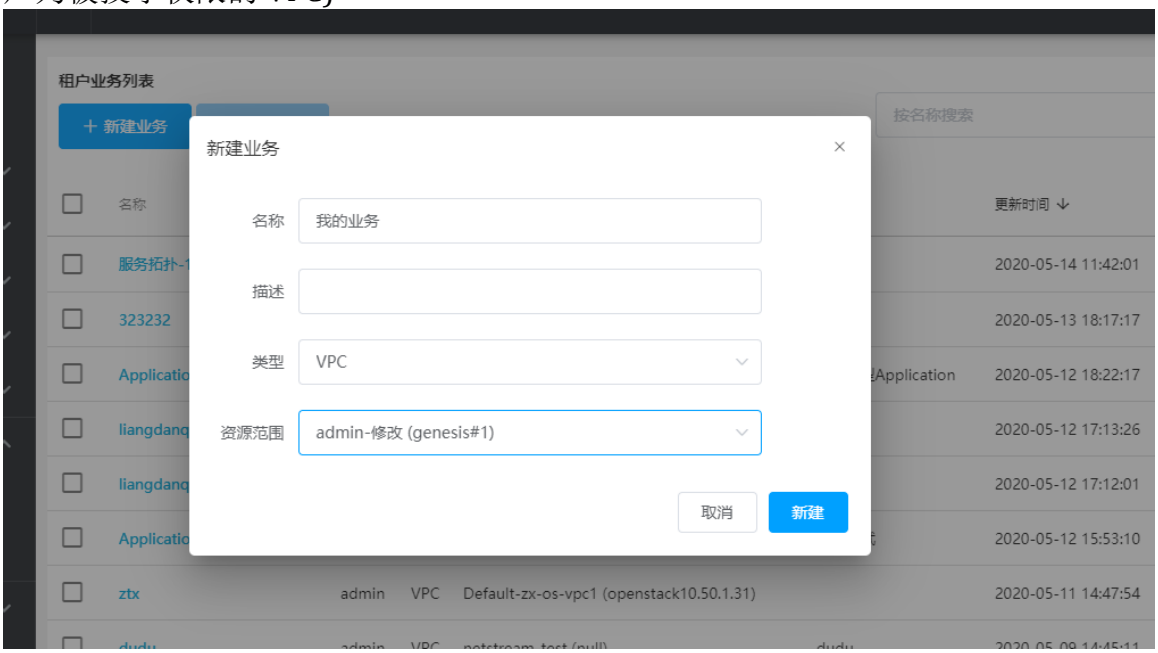
7.2.1 功能介绍

业务画像可将 VPC 或者子网的资源通过流量进行梳理，得到这组资源内部的应用服务依赖和流量访问关系，并可将这个关系通过业务、资源组、服务依赖保存下来，在全景图中查询对应的流量。

7.2.2 功能使用

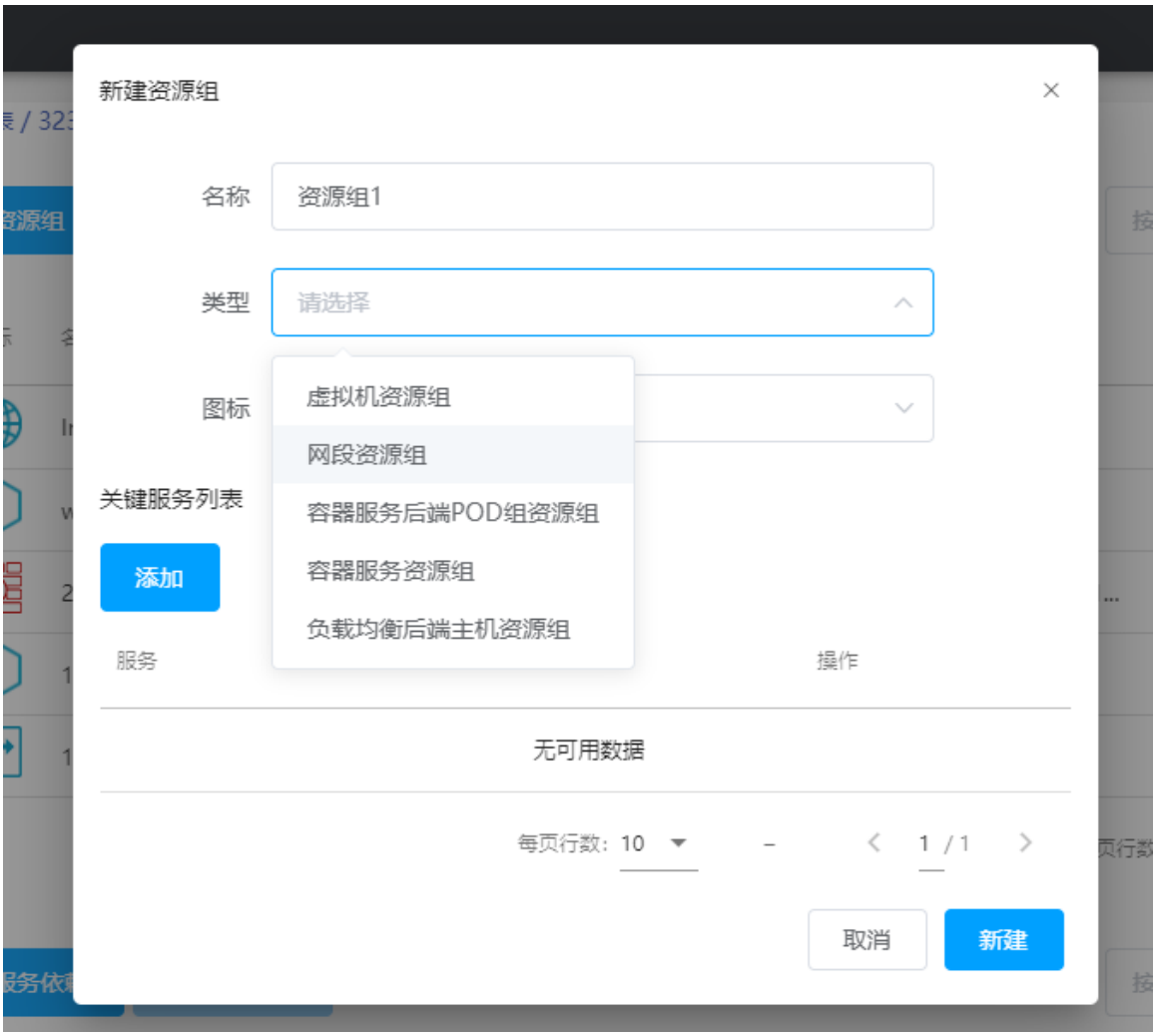
- 创建业务

  业务类型可以是 VPC 或者子网，对应的资源范围选择系统中的 VPC 和子网(用户为被授予权限的 VPC)



- 业务列表页可以完成对业务的修改和删除

- 进入业务详情页后，可以人工为业务中资源创建资源组



可以根据资源的实际属性，选择对应类型和图标。目前支持：

- 云服务器资源组，可选择业务内的若干云服务器。
- 网段资源组(子网类型业务只支持该类型资源组)，支持 IP 地址、IP 范围、IP 段的形式定义的网段资源。
- 容器服务资源组，可从业务范围中的容器服务中选择。
- 容器服务后端 POD 资源组，可从选择的容器服务的对应后端工作负载中选择。
- 负载均衡后端主机资源组，可从选择的负载均衡器的对应负载均衡策略中进行选择。

5.6.0 新增了关键服务列表，用于标记资源组关心的相关服务内容。其中，

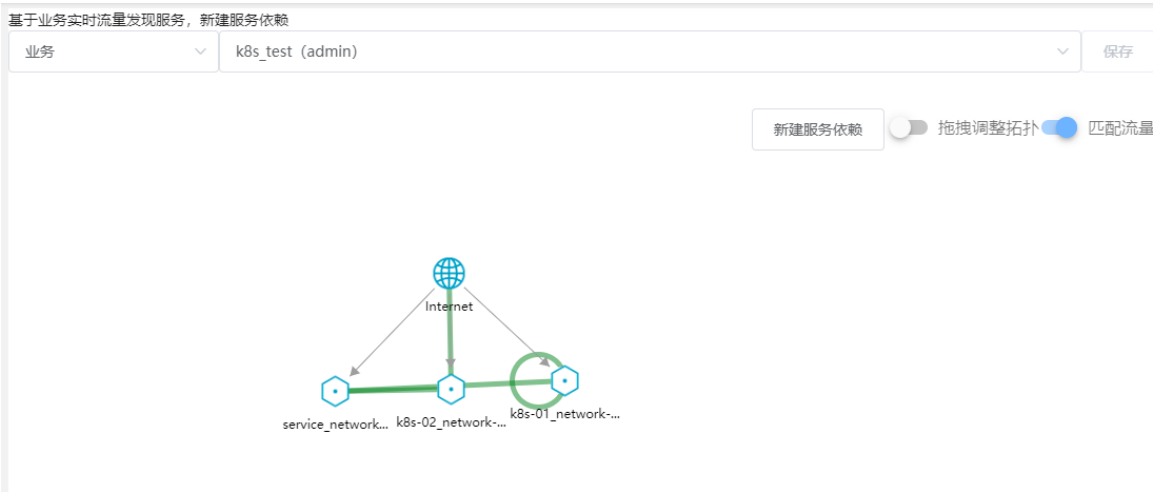
- 云服务器和网段类型资源组可以手动添加

- 容器服务类型资源组自动获取服务对外端口列表
- 容器服务后端 POD 资源组自动获取工作负载端口列表
- 负载均衡后端主机资源组自动从负载均衡策略中获取端口列表

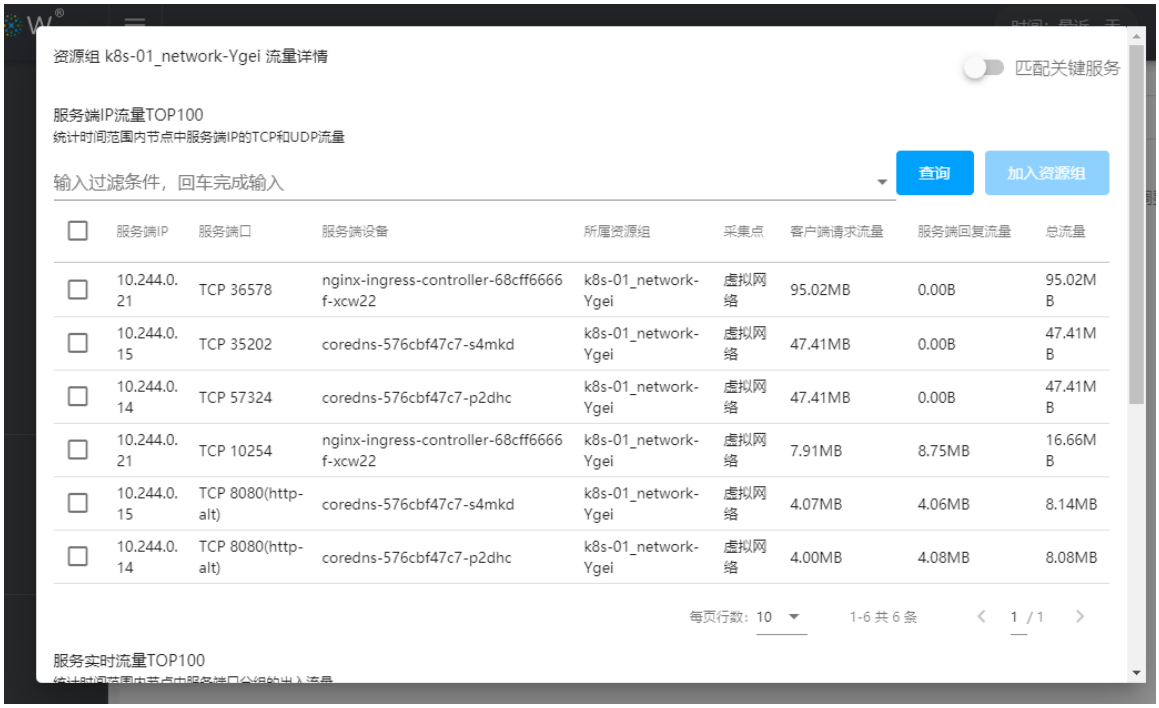
资源组之间可以通过服务依赖进行关联，描述资源组之间的依赖关系。

- 可以通过服务拓扑查看业务的拓扑结构以及实际的流量访问

- 支持查看业务，也同时支持 VPC 和子网，会自动生成一个临时业务，可在离开页面时保存业务。
- 服务拓扑可查看业务的服务依赖拓扑
- 可通过匹配流量开关，查看真实的流量叠加在服务依赖拓扑上的走向。

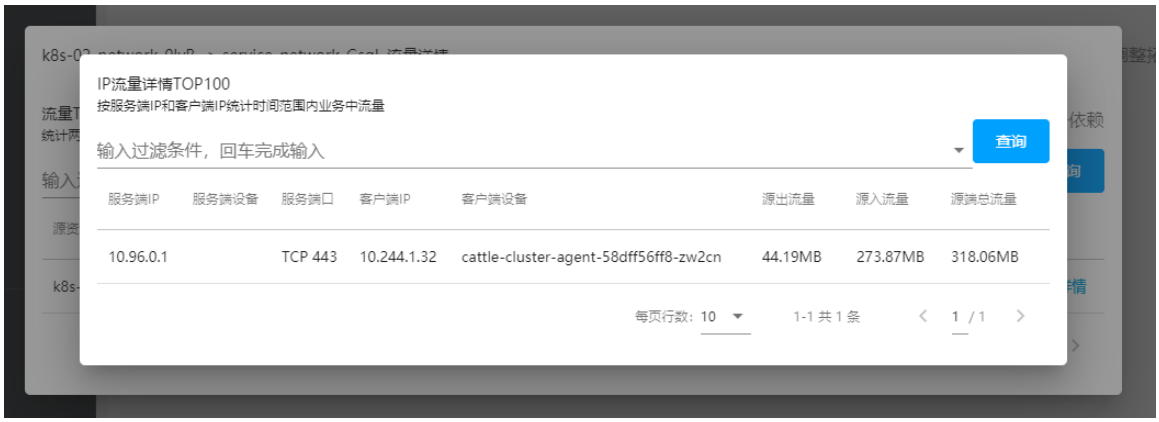


- 通过点击图中节点，可以查看对应的节点上的流量信息

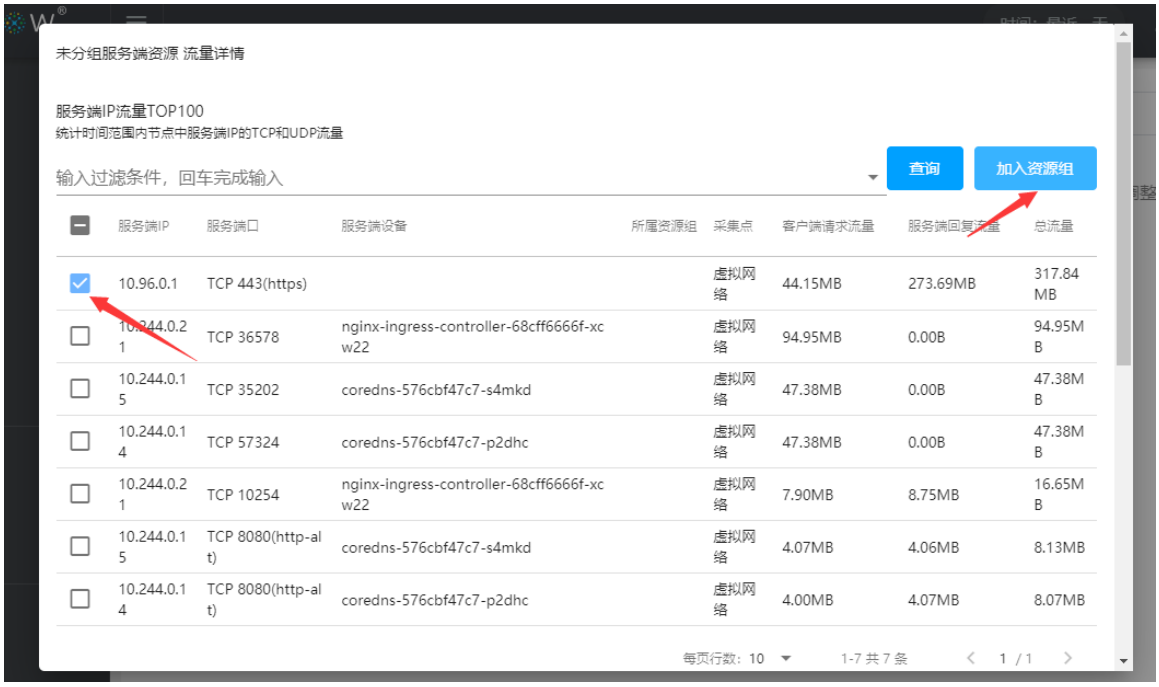


- 通过流量连线 tooltip，可以点击查看对应的服务依赖上的流量信息

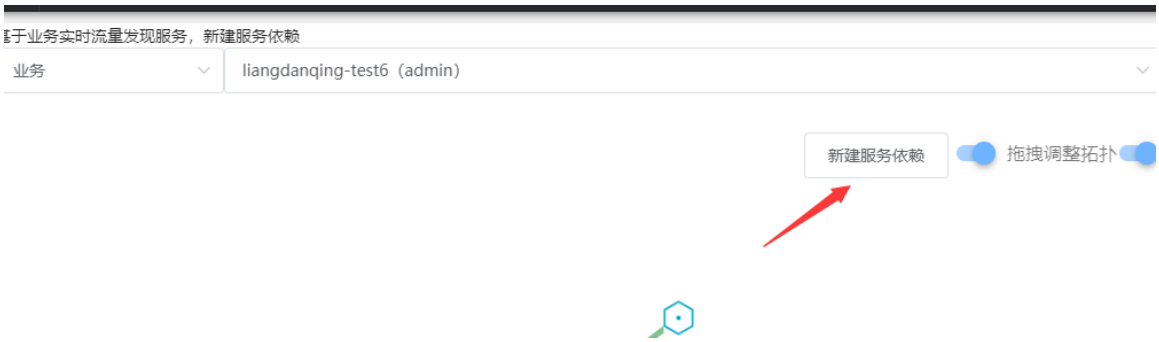
并可进一步查看两个资源组之间流量的详情



- 资源组(Internet 资源组除外)流量详情中，可以人工选择服务 IP 组成新的资源组，并可选择是否从现有资源组中移除。



- 也可以在服务拓扑中快速创建新的服务依赖



8. 系统

管理 DeepFlow 平台自身的组件、配置、软件授权、账号、日志等。

8.1 控制器操作

查看控制器列表信息：
- 状态：正常/异常两种状态
  - 监控是否有控制器失联，如果失联则认为异常。
- 角色：显示控制器的主、备、从角色
  - 主/备控制器：用于提供 Web 页面访问和 API 调用入口
- 操作：

- 配置导入/导出操作：主要用于备份恢复场景。
- 配置最大关联采集器数量：当采集器数量很大且控制器缺少 N+1 冗余时，避免控制器故障时对采集器进行切换，同时如果控制器资源规格不一致时，也可限制低资源控制器管理更少的采集器
- 配置 NAT IP：当从区域的控制器和数据节点通过 NAT IP 访问主备控制器时，可设置正确的 NAT IP 使得集群之间能正常访问，另外如果部分采集器需要通过 NAT IP 访问控制器也需要进行此项设置
- 设置为备：请选择主区域中的一个从控制器为备控制器，使得主备可以自动切换
- 设置运维：当 License 不够时多余的控制器会自动设置为运维，需要补齐 License 后才能取消运维
- 对于从控制器：支持设置其关联的区域和可用区，可用区可选择一个或多个，当可用区为空时表示为区域内所有可用区的采集器提供服务。
- 点击控制器名称，可进入详情页，展现控制器 CPU、内存、磁盘、系统负载等各项监控数据。

警告： 控制器配置导入仅用于备份恢复，导出后的配置不能进行修改，且不能导入到其他控制器上。

另外，通过界面可直接修改控制器的主要配置：
- NTP 服务器：需要设置为北京时间所在的时间同步服务器，产品页面上的所有显示时间都是以北京时间为基础。支持配置最多 4 个 NTP 服务器。另外，页面上支持查看控制器当前时间与访问者计算机的本地时间，可对比确定控制器时间是否准确。如果相差时长比较大，查看流量统计时可能产生时间错位，此时需要校准控制器或访问者计算机的本地时间。
- 云平台同步频率：需要根据云平台资源数量的大小设置合适的云平台同步频率，同步过快会给系统造成压力，同步过慢会导致系统的云平台数据与实际云平台数据差异过大，影响正常数据统计，展示等。通过查看云平台历史同步时间，能更优的设置云平台同步频率，建议云平台同步频率大于历史云平台同步平均时长。

8.2 采集器操作

8.2.1 查看采集器统计信息

根据总流量数据能清楚知道过去一天采集和分发的流量情况，根据曲线图清楚过去一天流量走势，根据谷值、峰值直观了解最近一天最小流量值与最大流量值：
- 最近一天采集流量：统计的为最近一天采集器从网卡捕获的流量
- 最近一天分发流量：统计的为最近一天采集器成功匹配分发策略，然后封装隧道报文头后的隧道流量
- 最近一天过滤流量占比：展示的为最近一天未分发流量的比例，由于分发流量需要增加隧道封装，该值可能为负数。计算方法为((采集总流量 - 分发总流量) / 采集总流量)* 100%。
- 峰值/谷值：统计的为最近一天流量曲线中的最高点和最低点

通过点击最近一天采集分发流量趋势曲线图，进入二级页面查看指定时间的采集流量、分发流量、过滤流量占比。可通过时间范围筛选需要查看时间段的数据历史曲线，也可自定义调整查看的时间粒度、调整自动刷新开关。

根据 TOP 5 采集器的 CPU、内存、运行环境负载情况，能清楚知道采集器对资源的消耗，可重点关注这些采集器所在运行环境（宿主机/云服务器）是否还能支撑采集器正常工作。

8.2.2 查看采集器列表

根据采集器列表，清楚知道采集器安装部署以及运行情况：

8.2.3 查看采集网卡列表

将采集器与控制器同步的网卡展示，方便管理

8.2.4 采集器组及配置

通过将相同类型的宿主机/云服务器归纳为一组，方便统一管理：
- 默认：如用户未给采集器自定义组，则都划分为默认组中。默认组不可能修改和删除。
- 采集器以最后加入的组为准。
- 全局配置：输入框为空时代表的系统初始值，将一个有值的框置空意味着还原为系统默认。高亮显示相对于系统初始值有变化的参数值 只能修改不能删除。
- 其他组配置：参数输入框为空时，表示使用采集器组的全局配置，高亮显示相对于全局配置有变化的参数值。
- 基础配置参数
  - 采集网口：
  - 采集包长：
  - 流量采集方式：
  - 解封装隧道类型：
  - 虚拟机 XML 文件夹：
  - 最长同步间隔：
  - 最长逃逸时间：
- 裸 UDP 最大 MTU：当使用裸 UDP 套接字传输数据时，如果采集器发送网卡的 MTU 不是沿途上的最小 MTU，需要在此进行配置。另外需要注意的是公有云上需要调低 MTU 至 1400 避免公有云篡改 UDP 大包的尾部字符。
- 全景图配置参数
  - 数据套接字：采集器发送指标量数据和流日志数据使用的套接字，默认为 UDP，可选择 TCP 提升传输可靠性（但是会占用更多的带宽资源）
  - PCAP 套接字：采集器发送 PCAP 数据使用的套接字，默认为 UDP，可选择裸 UDP 提升性能，也可选择 TCP 提升传输可靠性（但是会占用更多的带宽资源）
  - HTTP 日志代理客户端：默认为 X-Forwarded-For，为空时 HTTP 日志不提取代

理客户端 IP 字段，可自定义 Header - HTTP 日志 TraceID：可选项分别表示 Zipkin、Jaeger、Skywalking 使用的 HTTP Header，可自定义 Header
  - 应用层日志解析包长：采集 HTTP、DNS 日志时的解析的包长
  - 流日志采集速率(每秒)：每秒采集的流日志条数，超过时采样
  - 应用层日志采集速率(每秒)：每秒采集的 HTTP 和 DNS 日志条数，超过时采样
- 包分发配置参数
  - 分发套接字：采集器分发流量时使用的套接字，默认为裸 UDP，可选择 UDP 提升适配性（部分场景下使用裸 UDP 无法正确获取网关 MAC 地址）
  - 内层附加头：分发流量中是否添加内层 802.1Q 附加头，用于向第三方分析工具发送流量标签
- 基础功能开关
  - 同步资源信息：是否打开资源信息同步，用于在没有云平台资源信息 API 同步能力的场景下通过采集器同步 KVM 上的虚拟机、虚拟网卡、MAC、IP 等信息
  - 日志发送：开启发送功能，是会将采集器产生的日志都发送至控制器的 `/var/log/trident/$采集器.log` 目录下。如某台采集器出现异常时，又不方便登录采集器时，可直接将采集器的日志发送到控制器，在控制器集中查看定位原因。
- 全景图功能开关
  - 指标数据：采集器是否发送用于全景图的指标数据
  - 非活跃端口指标数据 - 应用层指标数据：采集器是否计算应用层指标数据
  - 流统计秒级数据：采集器是否发送全景图中的秒粒度流统计数据
  - 流日志数据：采集器是否发送全景图中的流日志数据
  - 过滤流日志：当不希望采集器发送所有采集点的流日志数据时，可配置采集点过滤列表仅发送对应采集点的流日志数据，一般用于降低流日志发送压力；默认为全部，表示所有采集点；为空时表示关闭流日志采集；
  - 过滤应用层日志：逻辑与过滤流日志类似，默认为全部
  - 包分发功能开关
  - 全局去重：当不希望采集器进行全局去重时，可关闭此开关

8.3 数据节点操作

8.3.1 数据节点列表

查看数据节点列表信息：
- 区域、可用区：数据节点关联的区域、可用区列表。数据节点会接收关联可用区中采集器的遥测数据、压缩包头和原始流信息并写入数据库或磁盘中。从控制器所在服务器一定是数据节点，通过设置从控制器关联的区域、可用区即可实现对数据节点的设置。
- 状态：正常/异常两种状态，主要监控是否有数据节点失联，如果失联则认为异常
- 关联采集器数量：目前关联的采集器数量
- 最大关联采集器数量：该值用于采集器切换数据节点时的超载保护。支持修改，输入值小于当前关联的采集器数量时，将会触发超出的采集器切换，被切换的采集

器进程将会自动重启。数据节点所在服务器上也会运行采集器，即最大关联数量至少为 1。
- 体系架构、操作系统、内核版本、总 CPU(核)、总内存：数据节点所处运行环境的系统信息。
- 点击数据节点名称，可进入详情页，展现数据节点 CPU、内存、磁盘、系统负载、队列丢包等各项监控数据。
- 操作
  - 设置运维：当 License 不够时多余的数据节点会自动设置为运维，需要补齐 License 后才能取消运维
  - 配置区域和可用区：支持设置其关联的区域和可用区，可用区可选择一个或多个，当可用区为空时表示为区域内所有可用区的采集器提供服务。
  - 配置最大关联采集器数量：当采集器数量很大且数据节点缺少冗余时，避免数据节点故障时对采集器进行切换，同时如果数据节点资源规格不一致时，也可限制低资源数据节点管理更少的采集器
  - 配置 NAT IP：如果部分采集器需要通过 NAT IP 访问数据节点，需要进行此项设置
  - 配置参与聚合：当同一个区域内数据节点无法全部互相通信时，可以将其中某个可用区的数据节点设置为参与聚合，其他可用区仅需要和此可用区内的数据节点通信而无需相互通信

8.3.2 存储配置

全景图统计数据分为流统计、流量日志两种数据库，分钟粒度数据默认保存 1 周、秒粒度数据默认保存一天，过期数据自动删除。用户可基于已有的数据源自定义新的数据源，最多支持 10 个数据源。点击每个数据源，可查看数据的磁盘占用总量、每个时间间隔的占用增量、所在磁盘的剩余空间，用户可据此设定合适的保留时间。

网络诊断中 PCAP 数据默认保存 1 周，1 周以前的数据会自动删除。该页面展现统计数据的磁盘占用总量、每个时间间隔的占用增量、所在磁盘的剩余空间，用户可据此设定合适的保留时间。

系统中的监控数据默认保存 1 周，1 周以前的数据会自动删除。该页面展现监控数据的磁盘占用总量、每个时间间隔的占用增量、所在磁盘的剩余空间，用户可据此设定合适的保留时间。

8.4 账号管理

账号支持多个管理员、多个租户，管理员之间权限一致，租户可被管理员授予不同资源的查看权限。

- 管理员列表
  - 超级管理员可以增删改查所有管理员账号及租户账号
  - 非超级管理员只可修改自己的账号

- 租户列表
  - 管理员可以增删改查授权所有租户账号
  - 租户只可修改自己的账号
  - 租户可被授权的资源有：
    - VPC，及 VPC 相关的云服务器、VPC、子网、路由器、DHCP 网关、IP 地址、NAT 网关、负载均衡器、云数据库 RDS、云数据库 REDIS
    - 容器命名空间，及命名空间关联的 Ingress、服务、工作负载、ReplicaSet、POD
  - 租户可看到的目录有：
    - 全景图（流量搜索、流量下载）、视图（视图列表）、告警（告警策略、告警事件）、报表（报表策略、报表下载）、资源（所有页面）、系统（账号管理）