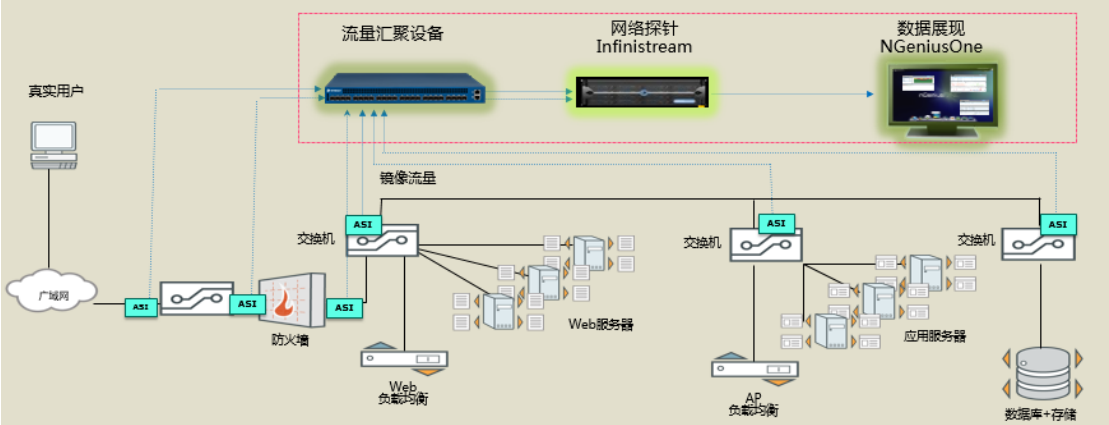
NETSCOUT

nGeniusONE 操作手册

目录

1. 组成和工作原理

NETSCOUT 网络流量分析系统主要由 Infinistream 网络探针和 nGeniusONE 管理服务器（可通过浏览器登录使用）共同组成。



1.1 系统组成

1.1.1 Infinistream 网络探针

Infinistream 设备（以下简称探针）通过交换机镜像或分光器的方式旁路接入网络监听网络数据，存储所有网络数据包的同时并对所获取的数据包信息进行统计分析，统计结果临时驻存于内存中。nGeniusONE 管理服务器会定期发送指令收取探针的统计数据，并将数据长期保留 nGeniusONE 服务器的数据库中用于长期的调用查看。网络探针在对包头信息进行统计分析的同时，还存储原始数据包至探针的高容量存储介质，并可在需要进行快速的、支持丰富过滤条件的数据包挖掘和输出。

1.1.2 nGeniusONE 管理平台

nGeniusONE (以下简称 nG1)是系统的统一管理平台和核心监控软件，安装在服务器上，配置探针的分析策略，收集探针采集到的信息，并进行汇总、分析。实现统一的、相互

关联的网络性能监控分析。

运维人员通过浏览器远程登录 nG1 服务器的进行管理配置和分析，nGeniusONE 的主要功能如下：

- 对单个或多个网络探针进行全局的配置
- 用于流量和应用的监控、分析和故障诊断
- 记录所有统计数据
- 内置数据库
- 同时实现实时性监控与自动化历史数据分析

1.2 主要特点

（1） 零风险接入

采用旁路方式接入网络，可在不改变网络的拓扑结构的前提下实现对网络流量的监控。对生产网络及应用系统无任何影响。

（2） 提供丰富的网络、应用性能相关的参数指标

网络流量分析系统可实现网络 2-7 层的监控分析，从链路层、网络层到应用层，针对链路、主机、主机组、会话、应用等对象，提供丰富的网络性能相关的参数指标，如吞吐量、网络连接时间、TCP 健康状况等信息。提供丰富的应用性能相关的参数指标，如应用流量、服务器延迟、应用响应时间及分布、应用会话数量、应用错误统计等信息。

（3） 高密度监听接口

设备提供高密度的监听接口，使用单台设备即可对多条线路/节点实现监控。在满足分析性能的前提下，可充分利用接口资源，投资效益最大化。

（4） 高精度流量分析

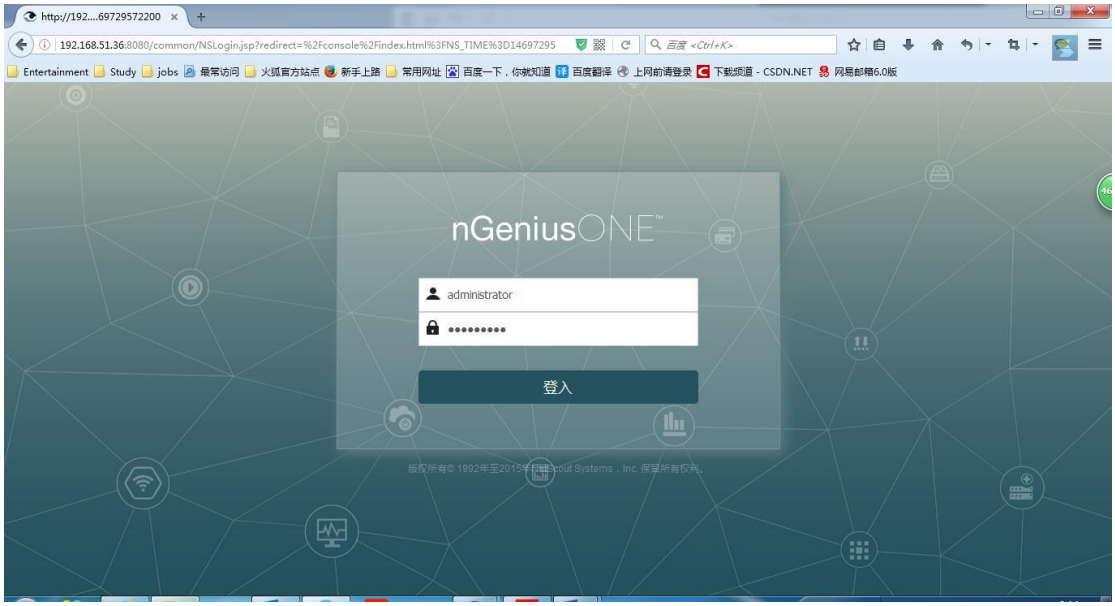
网络流量分析系统可对流量实现高精度的监控和分析，可提供秒级实时流量监控、毫秒级的突发流量分析，以及分钟级的长期历史流量分析。

（5） 原始数据包记录

探针提供大容量的存储，可记录原始数据包，并提供纳秒的数据包时间戳，用于对流量进行高精度分析和对异常/故障数据的回溯分析，故障定位。

2. 系统登录方式

nGeniusONE 的主要操作都通过浏览器方式，在浏览器中输入 nGeniusONE 服务器的 IP 地址和服务端口 xx.xx.xx.xx:8080，输入用户名和密码，点击登录



登录后界面

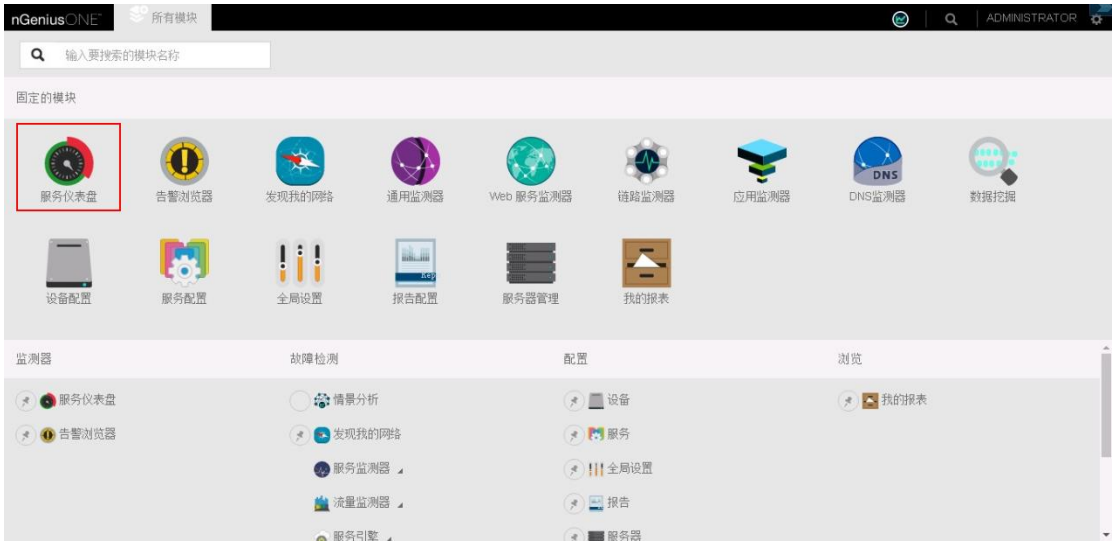
3. 重要功能介绍

3.1 日常监控

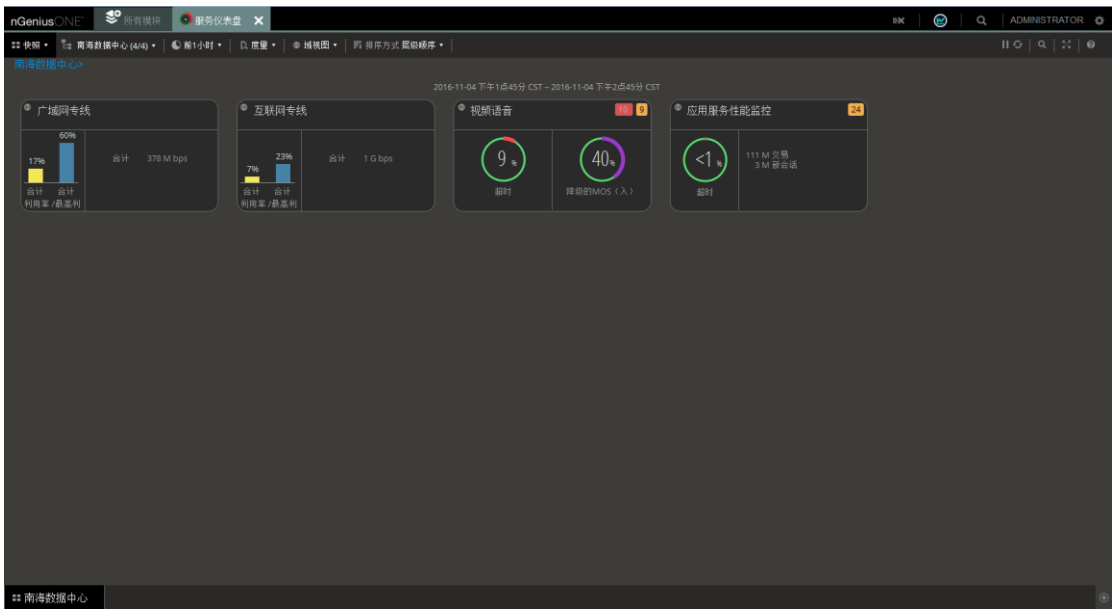
对模块进行定制后，可直观便利地观察到业务的实时状态，协助运维人员及时发现网络中的故障以及根据当前状态预见即将出现的风险。

3.1.1 服务仪表盘

在“所有模块”界面点击“服务仪表盘”进入服务仪表盘。



服务仪表盘（Dashboard）一般作为监控应用服务的入口，其可以显示应用的失败率、交易量、新会话、告警，链路的当前利用率、包率等信息。



仪表盘按层级显示，点击服务仪表盘右侧的  按钮可查看整个服务层级

每个仪表盘代表一个应用系统的服务质量 KPI，以下图为例：

这个服务代表“应用服务性能监控”应用（已事先在“服务配置”中定义）；

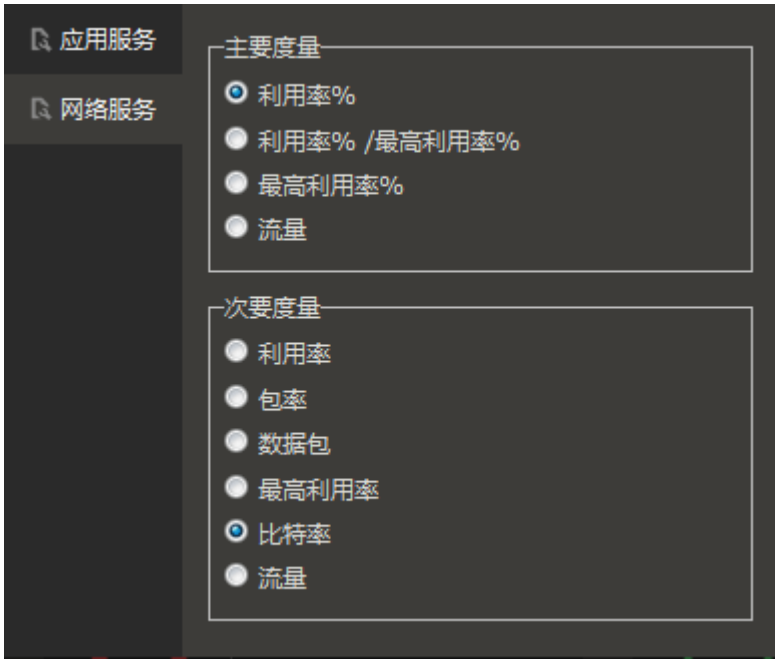
圆圈内的数字代表有<1%的超时率（圆圈颜色绿色表示交易正常，红色表示有交易失败）；

右边的数字上方表示有 111M 个交易数量，下方表示有 3M 个新建会话数量。

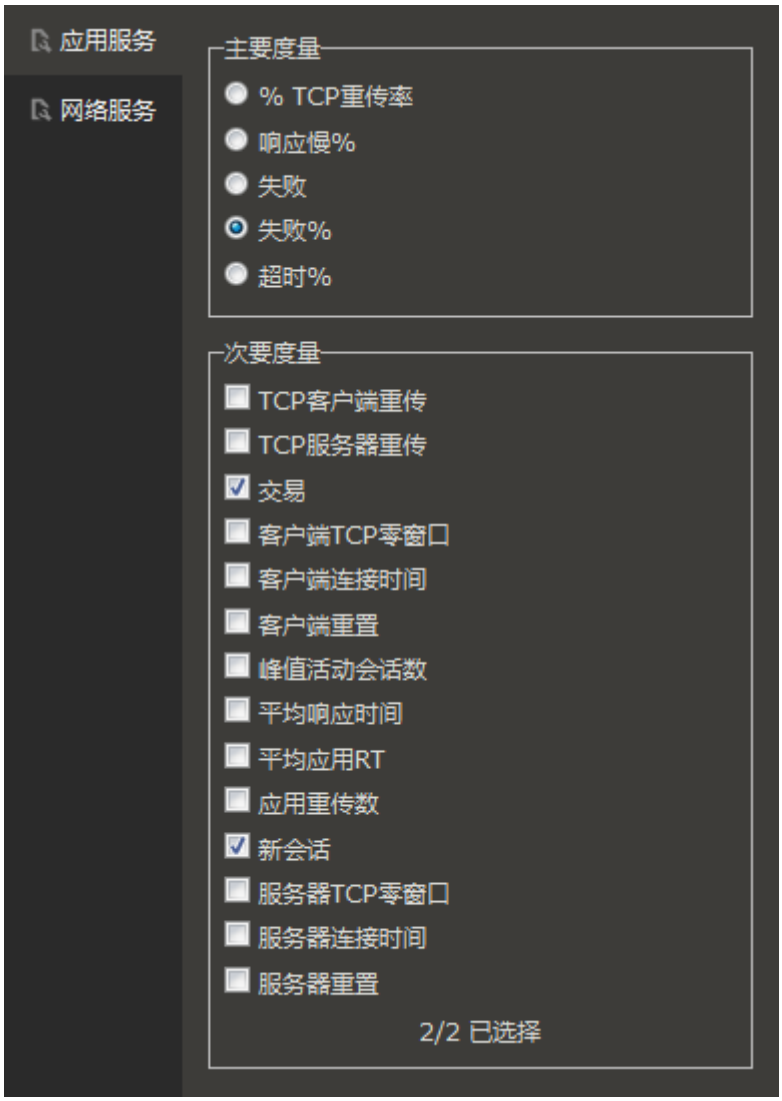
仪表盘上展示的指标可以在左上方的 

进行更改，对于网络服务和应用服务有不同的参数供选择

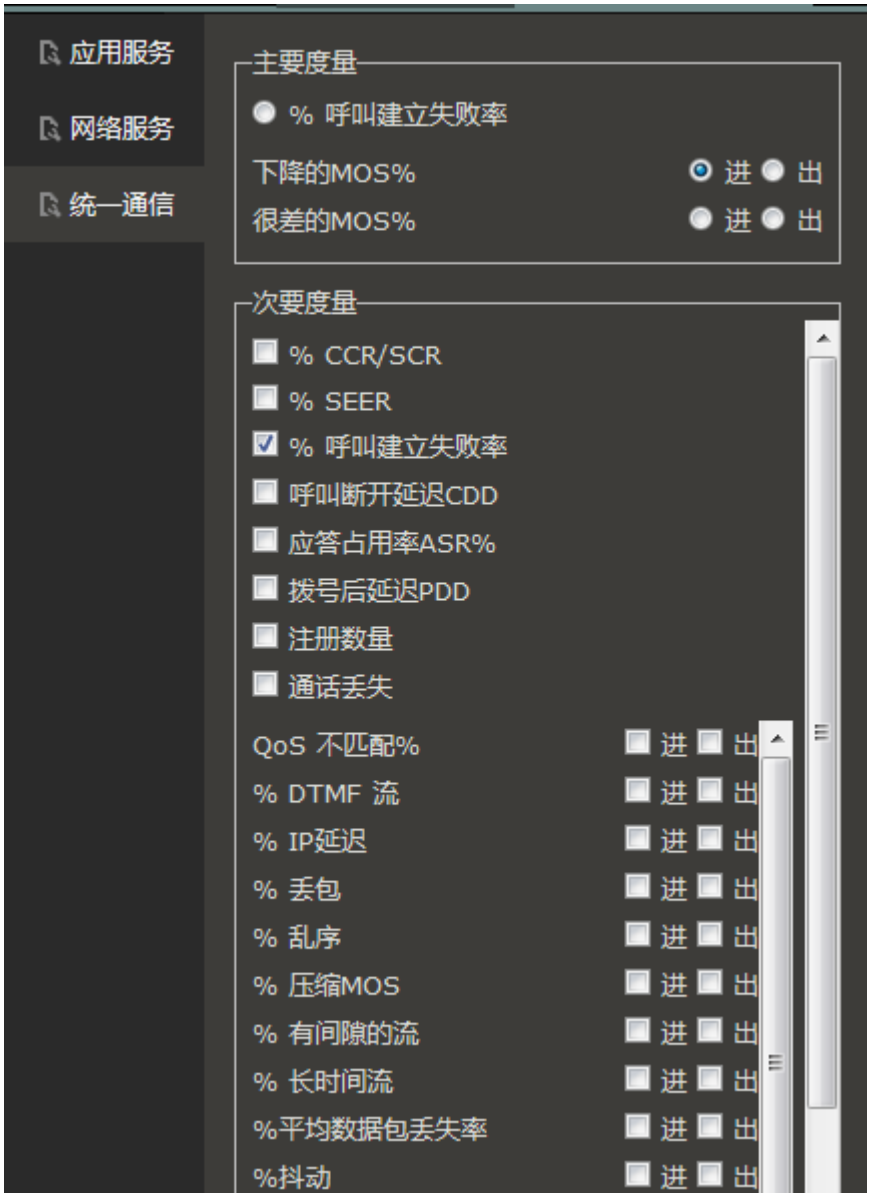
网络服务：



应用服务：


应用服务
网络服务
主要度量
% TCP重传率
响应慢%
失败
失败%
超时%
次要度量
TCP客户端重传
TCP服务器重传
交易
客户端TCP零窗口
客户端连接时间
客户端重置
峰值活动会话数
平均响应时间
平均应用RT
应用重传数
新会话
服务器TCP零窗口
服务器连接时间
服务器重置
2/2 已选择

统一通信：



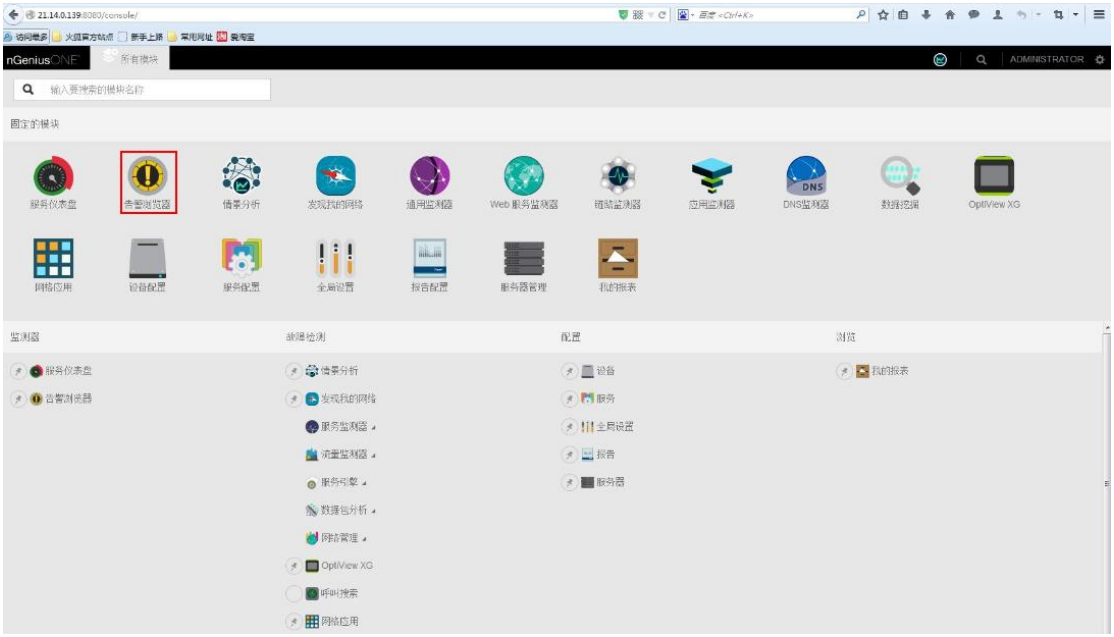
进入到各个模块的最底层后，点击左上角的  ，可以选择展示“快照”和“曲线”两种模式。“快照”模式下指标以数字形式展示，“曲线”模式下指标以图表形式展示

曲线模式

3.1.2 告警浏览器

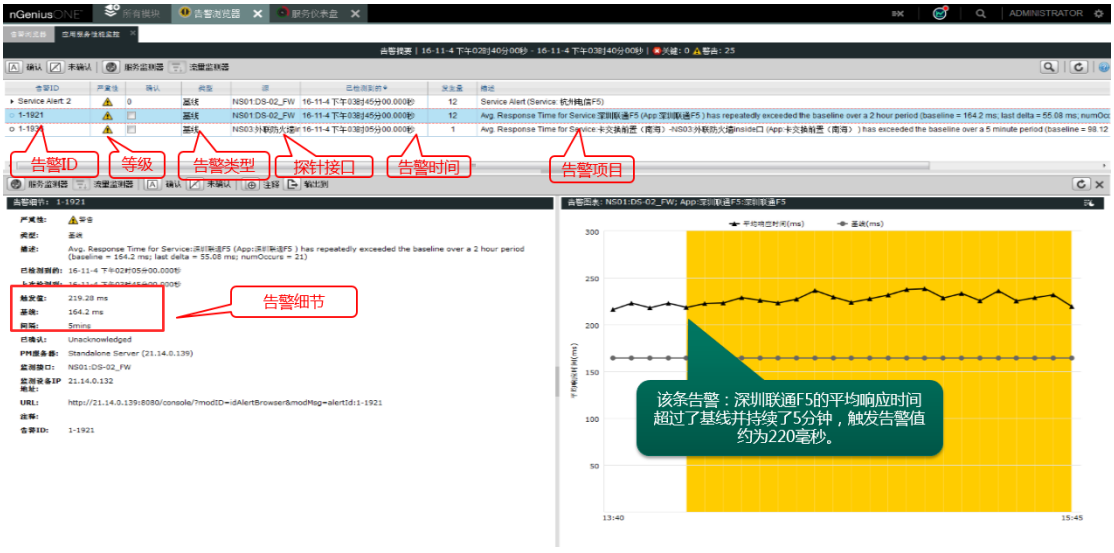
当出现告警时，在服务仪表盘上能看到仪表盘上显示了告警数量以及告警级别（橙色代表警告级别，红色代表严重级别）。

或在 nGeniusONE 界面图标栏点击“告警浏览器”，查看历史告警信息，如下图所示：

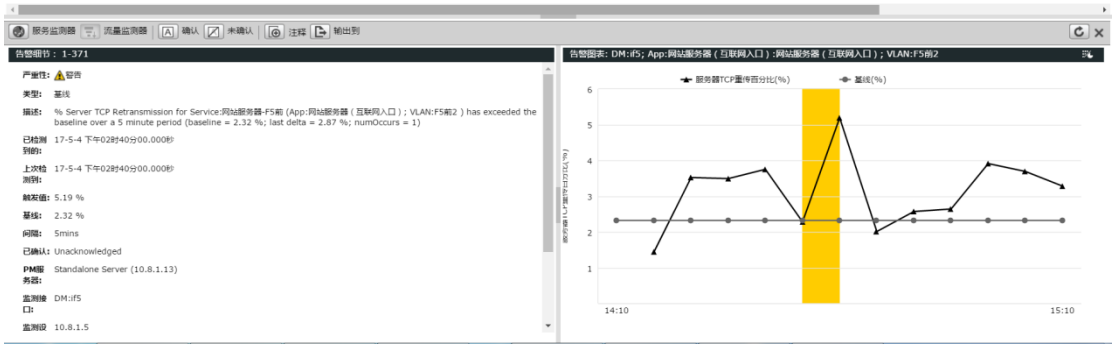


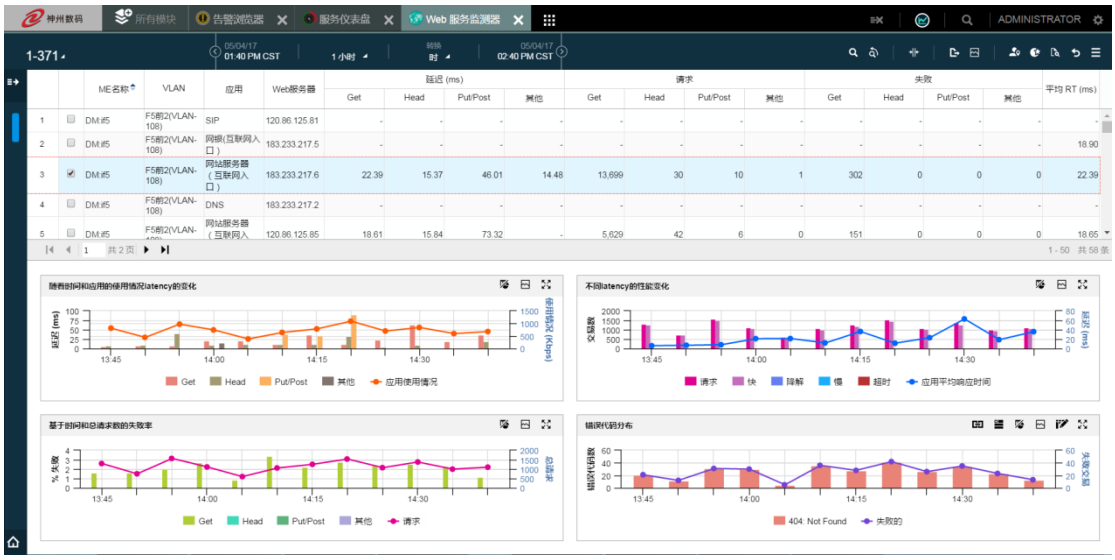
在告警浏览器中可以对基线告警和阀值告警产生的告警事件进行查看，如下图所示：

应用服务“深圳联通”的平均响应时间超过了基线值，因此 nGeniusONE 产生了告警。在该界面分别有对告警细节的详细描述以及以曲线图形式展示告警持续时间



从告警浏览器中可以直接跳转到服务对应的监测器中，如下图中的 1-321 告警，点击上方服务监测器按钮，可进入到该服务对应的监测器中

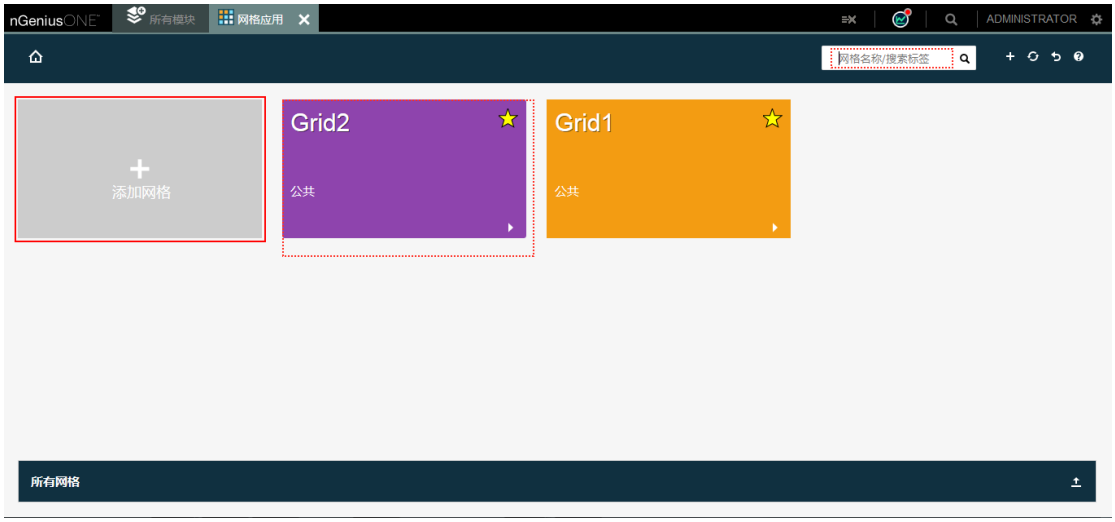




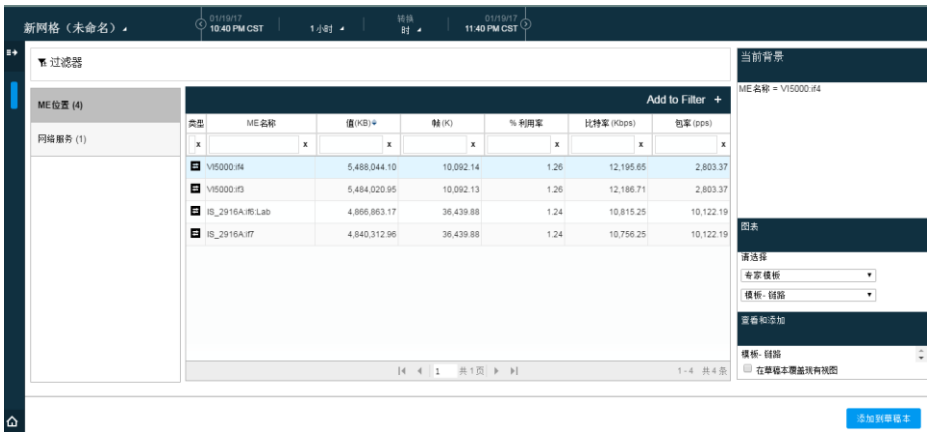
3.1.3 网格应用

网格应用将需要查看的信息长期保留在面板，方便需要的时候调出查看，无须再手动添加界面。

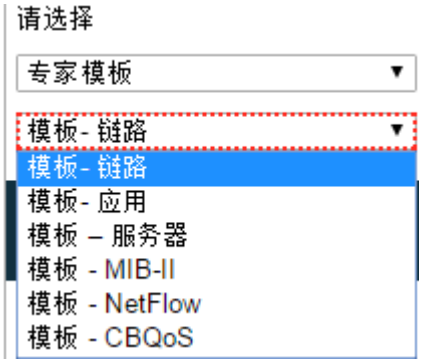
首先添加一个新的网格，点击添加网络，进入定制新网格的界面



选择监控对象以及模板：

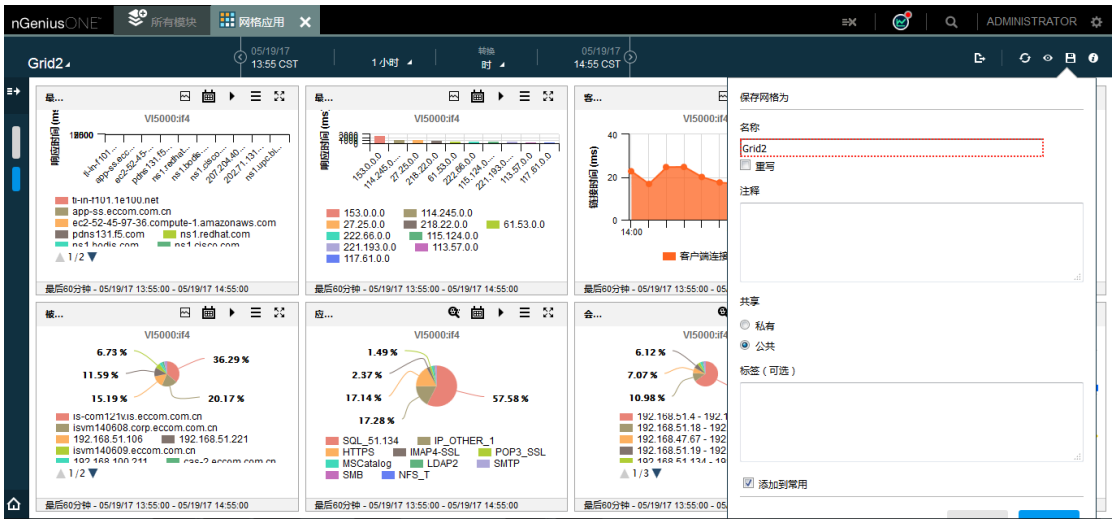


有多种已定义好的“专家模板”供用户直接调用

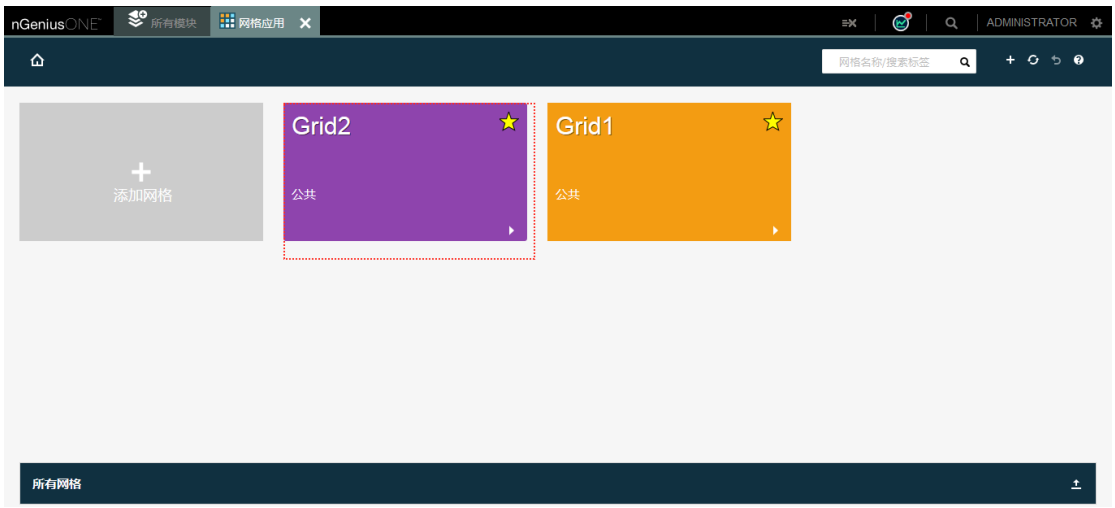


或者由用户自己选择监控指标，创建“单一视图”，有丰富的指标供用户选择

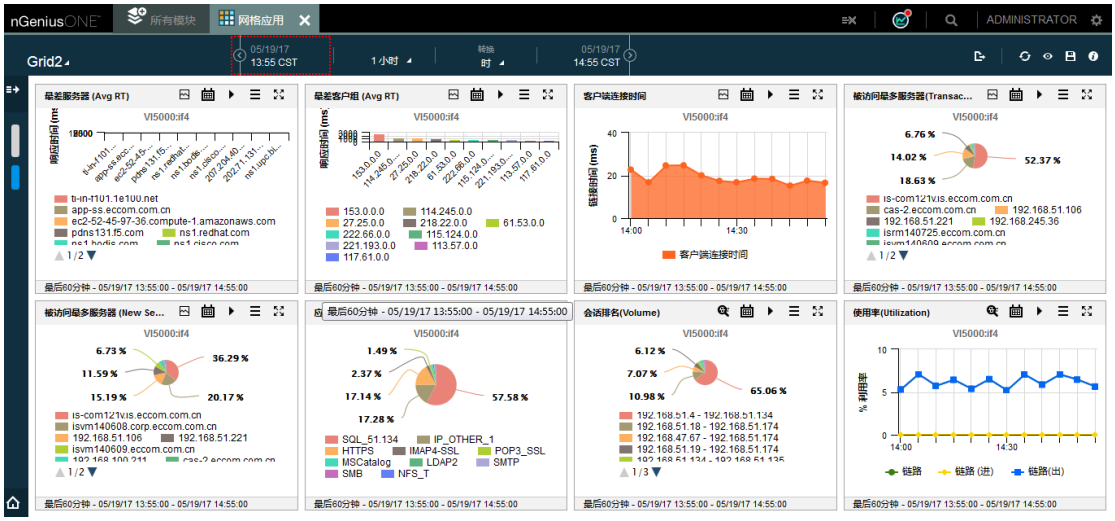
将视图添加到网格中并保存



定制好的网格保存在首页中，点击相应网格便可查看定制在面板上的信息

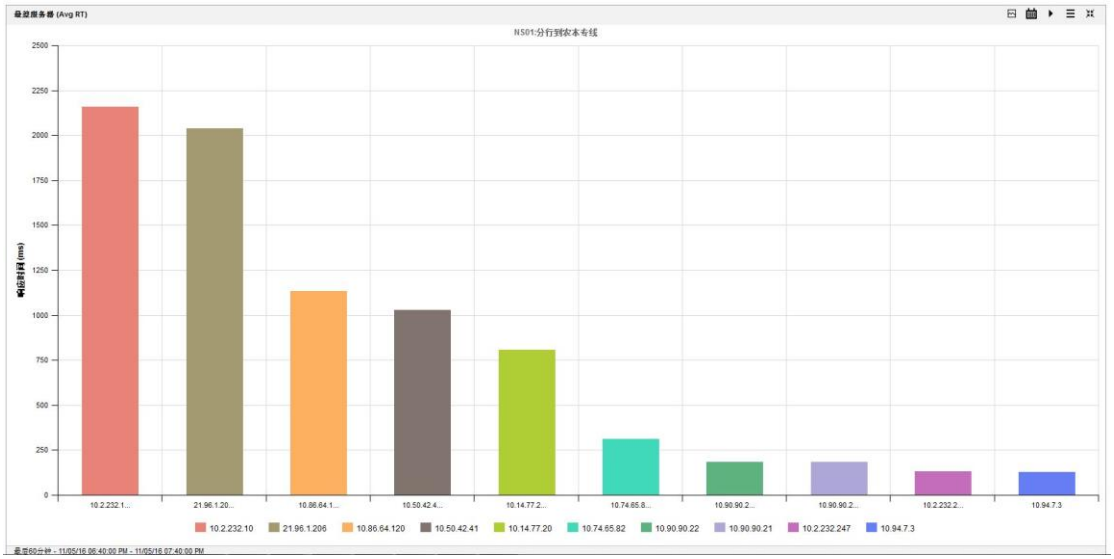


面板中的各个信息模板可实时更新，方便运维人员关注重要业务的实时动态

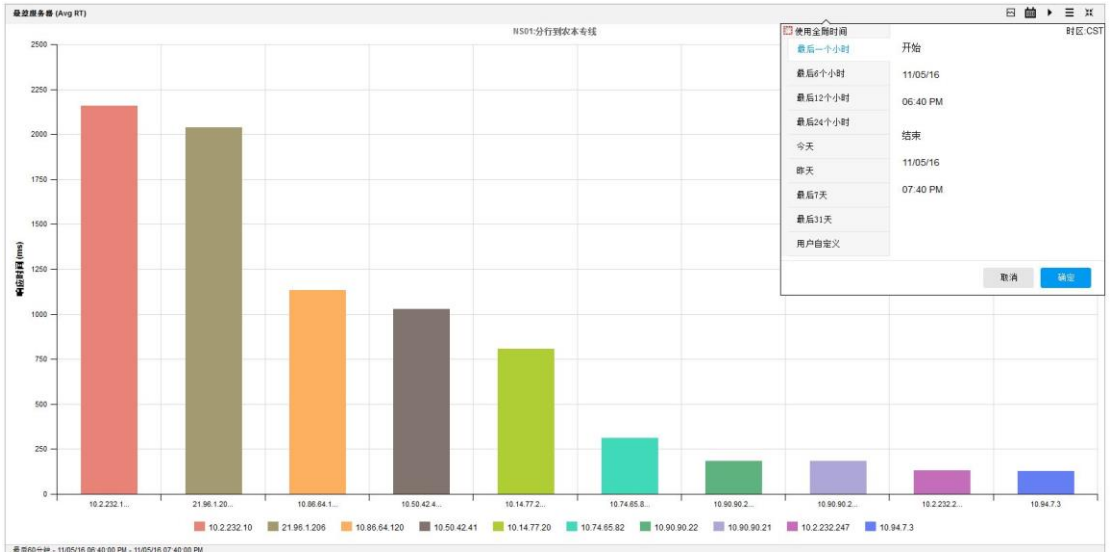


对于面板内的每个模块，我们可以进行如下操作：

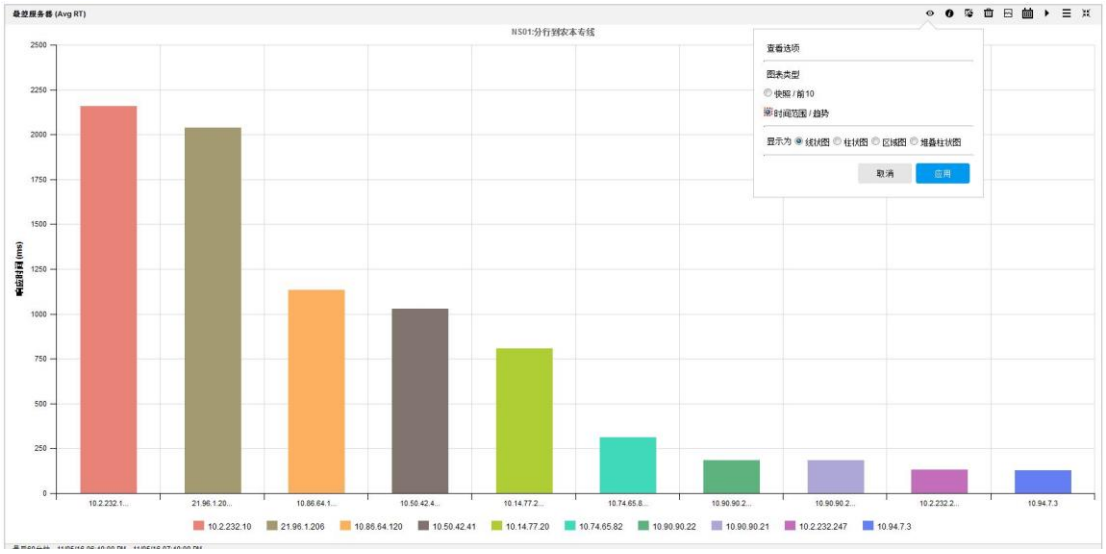
①，将单个模块放大至全屏



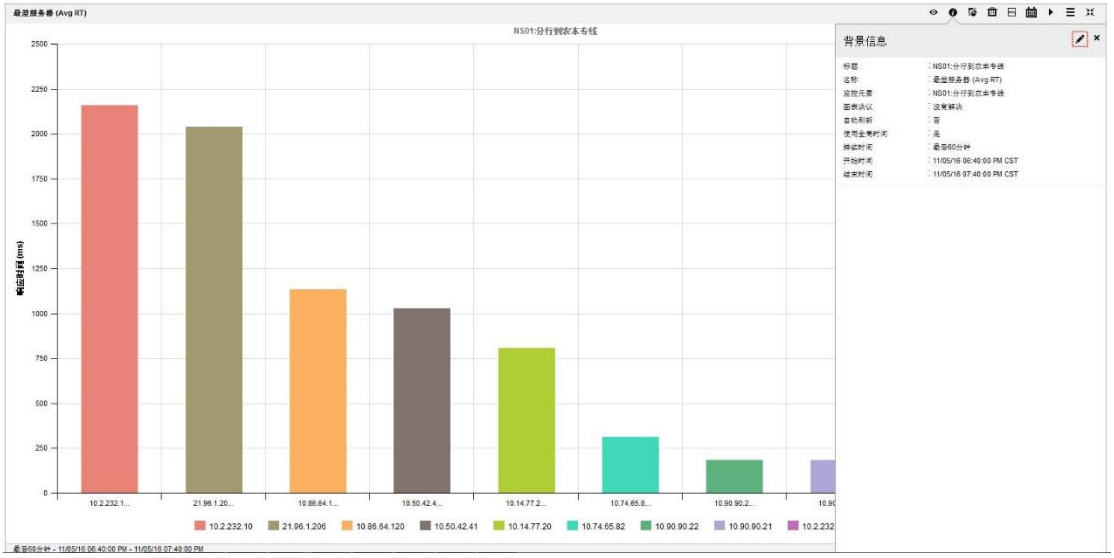
①  ，更改查看时间



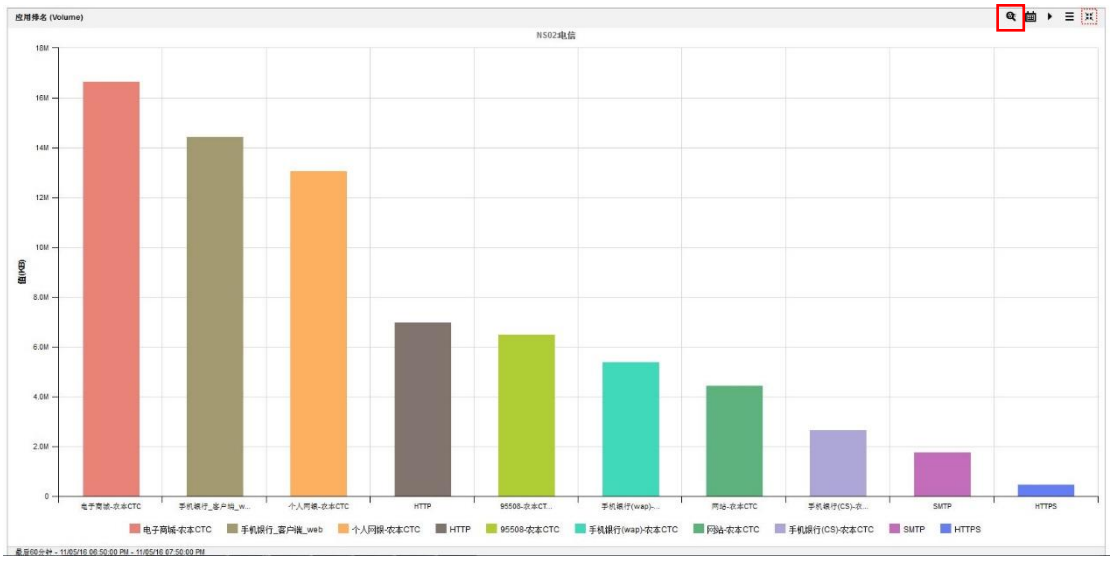
②  ，更改查看选项，如将柱状图改为曲线图、饼状图等

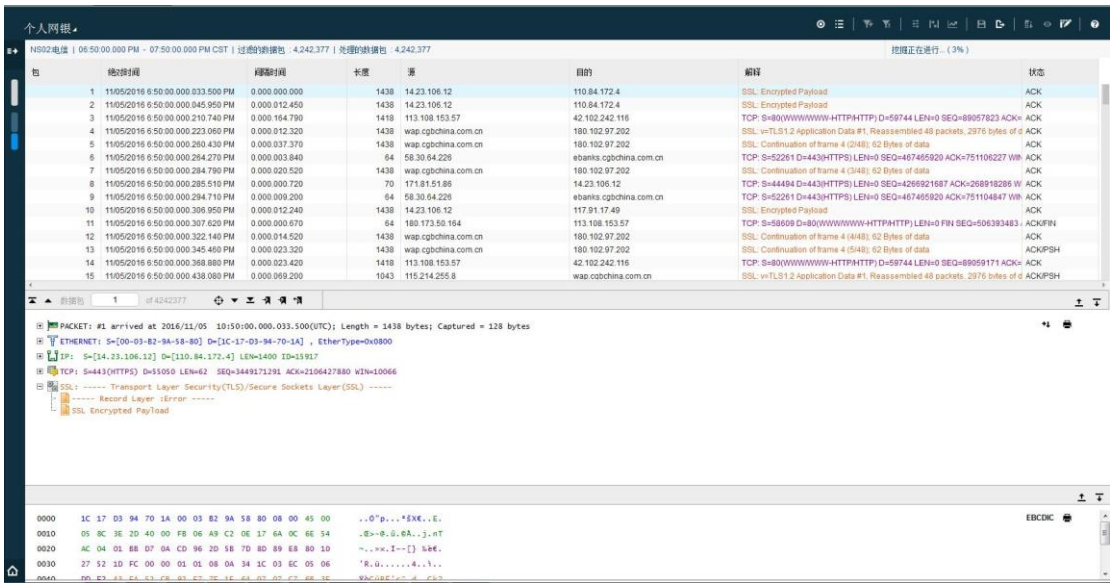


③  ，查看背景信息，查看模块的详细信息



④  ，数据包解码，对模块监测的时间段探针捕获的数据包进行解码





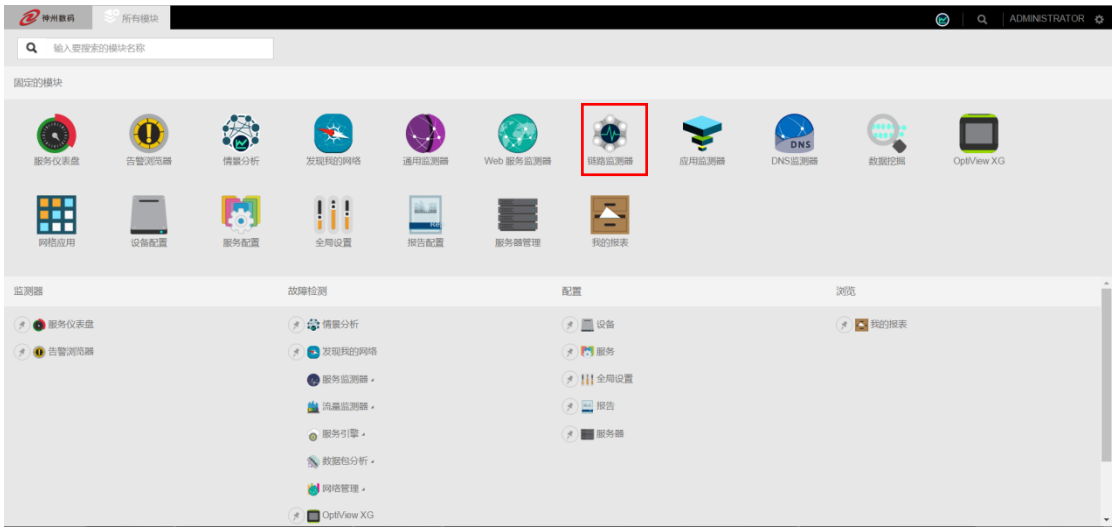
3.2 流量监测器

3.2.1 链路监测器

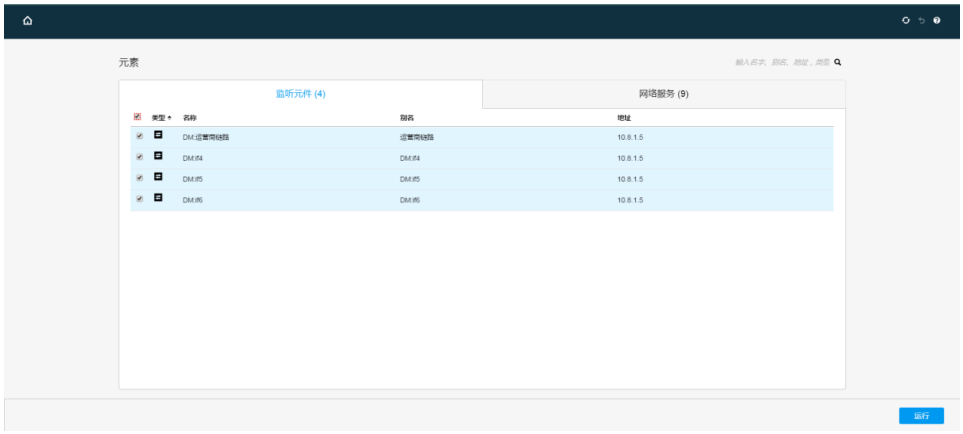
链路监测器，可用于查看链路实时流量，包括吞吐、包转发、平均流量、突发流量等，同时具备多个模式，用于查看不同种类的流量以及流量中的应用成分。

① 界面介绍

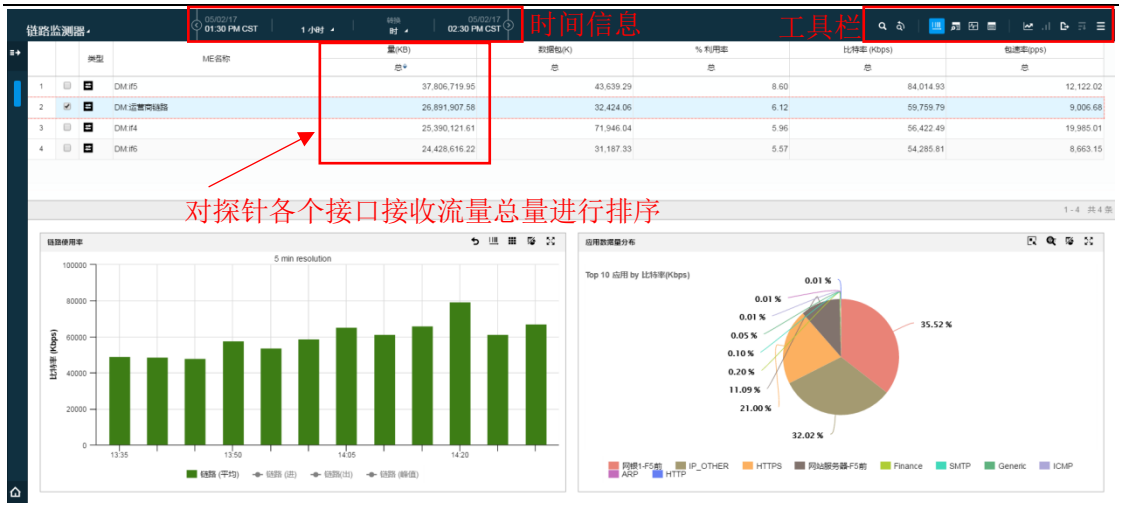
从所有模块中选择“链路监测器”进入链路监测器。



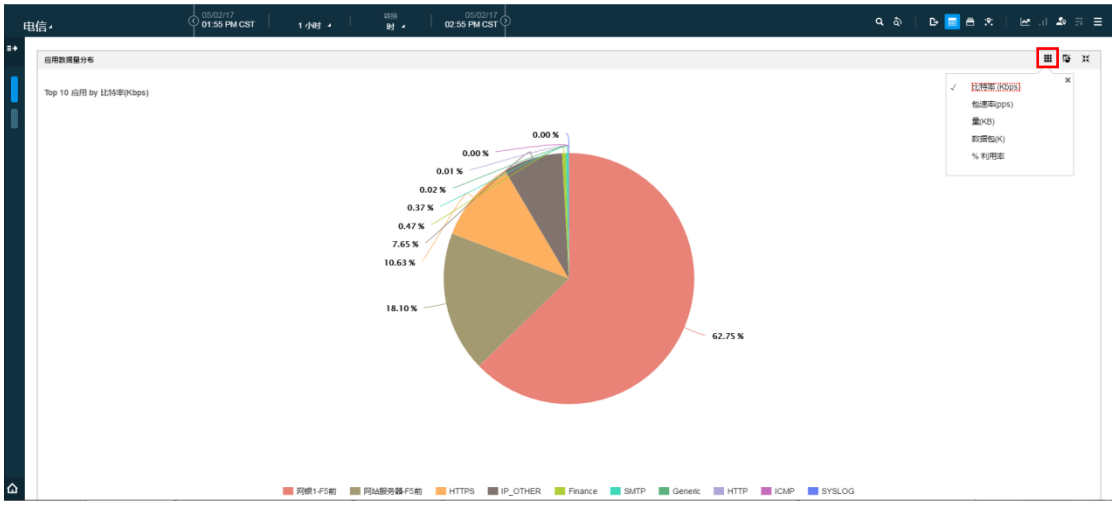
选择需要查看的接口（此处全选），点击“运行”后进入监测器。



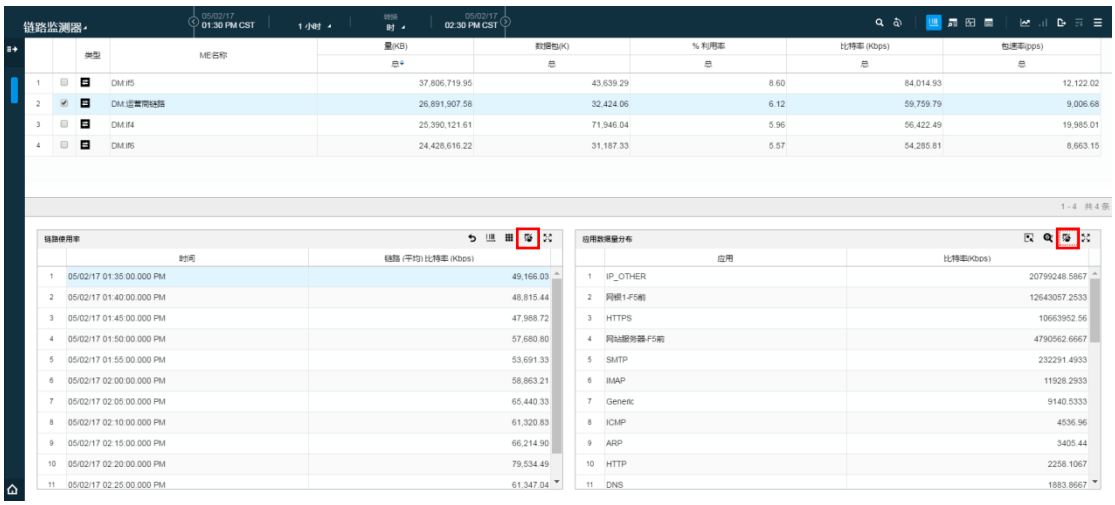
在监测器界面的顶部能看到当前查看的时间信息以及监测器工具栏（各个监测器均有此项，后面不再累述）。界面上半部是流量信息表格，可查看该时段内流量的总量、数据包数量、比特率、包率以及利用率；左下方是流量信息按时间分布的比特率柱状图，右下方是流量中比特率 TOP 10 应用分布的饼状图。另外，点击上半部表格中的某一列，可对该列进行排序，如下图中对探针接口接收的字节总量进行了排序。



除了查看比特率外，还可以点击  按钮对查看对象进行更改，可查看包率、流量总量、数据包数量、利用率等信息。

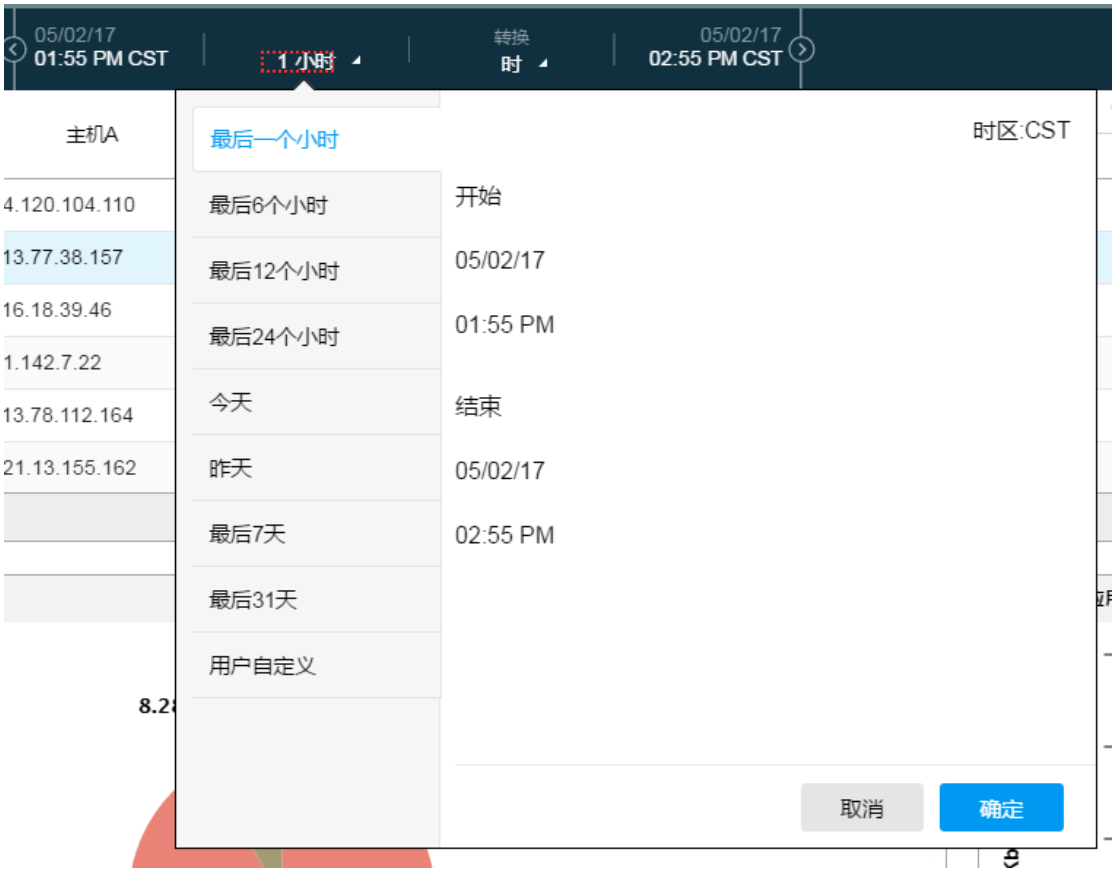


点击  按钮，可将图表信息转换成表格显示



可以对查看时间段进行更改，有“最后一个小时”、“最后 6 个小时”、“过去 7 天”等时

间段可选择，也支持用户自定义查看时间段。选择想要查看的时间段，然后点击“确定”完成选择。

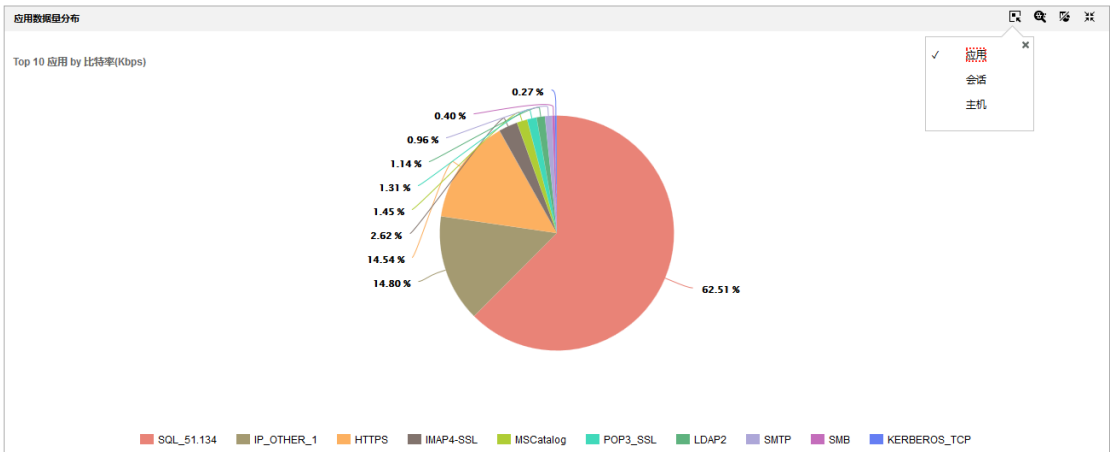


在此界面中还有如下参数可添加查看：

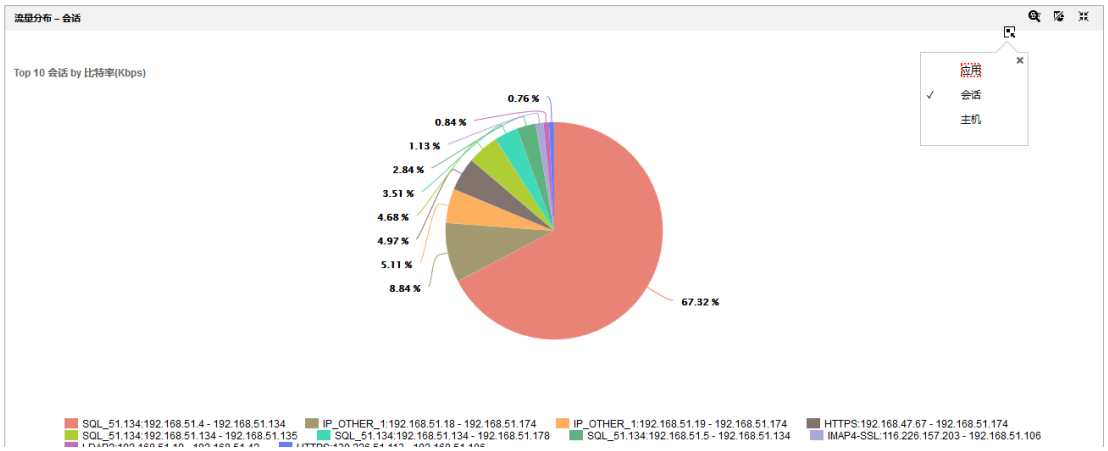
② Top 10 应用、应用层通信对以及应用层主机

在链路监测器中可查看 Top 10 应用、应用层通信对以及应用层主机信息，点击饼状图右上方的按钮，选择“应用”、“会话”或“主机”来选择想要查看的对象。

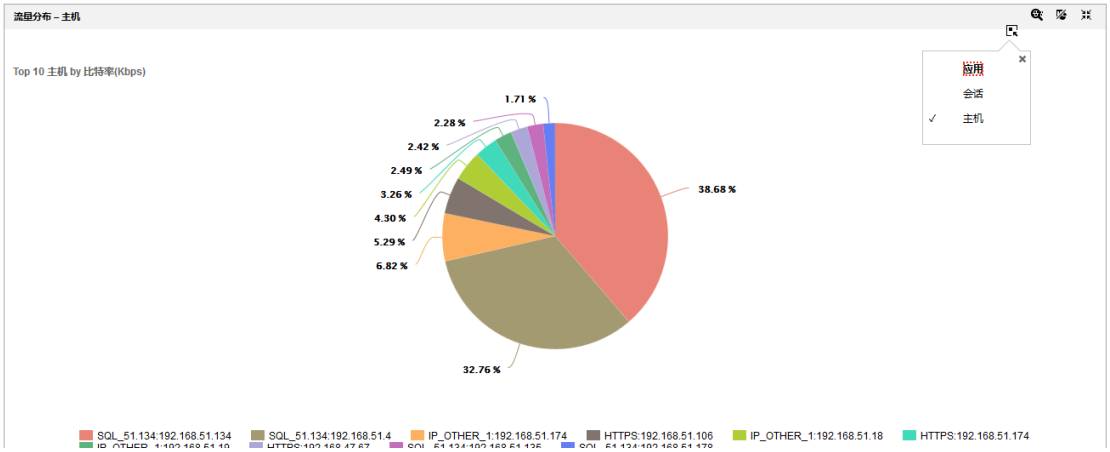
Top 10 应用：



Top 10 应用层通信对：能看到通讯对 113.78.190.139-117.136.40.39 的比特率占比最大



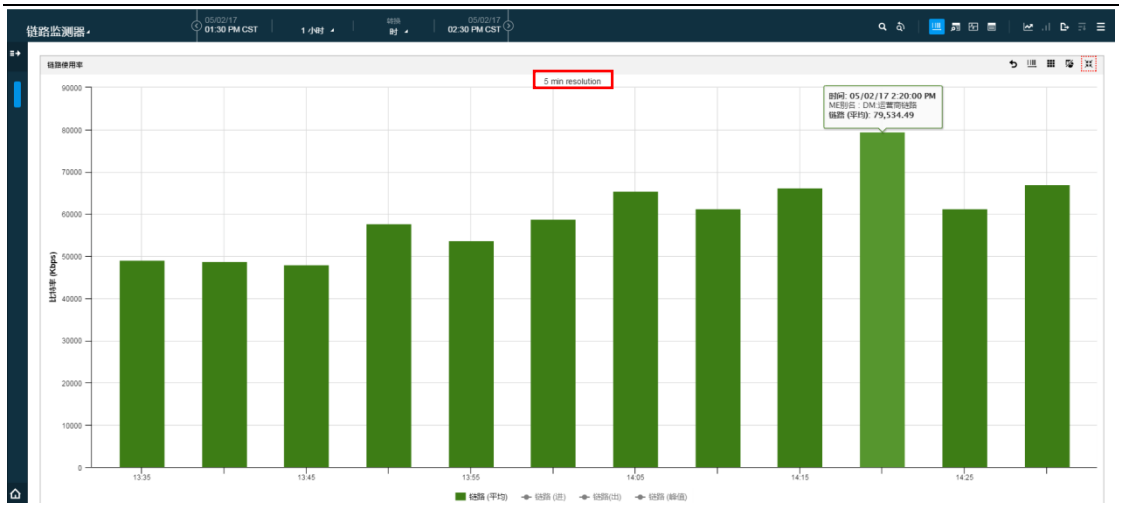
Top 10 应用层主机：可以看到地址 218.16.101.74 的比特率占比最大



③ 精确至毫秒级的链路监测

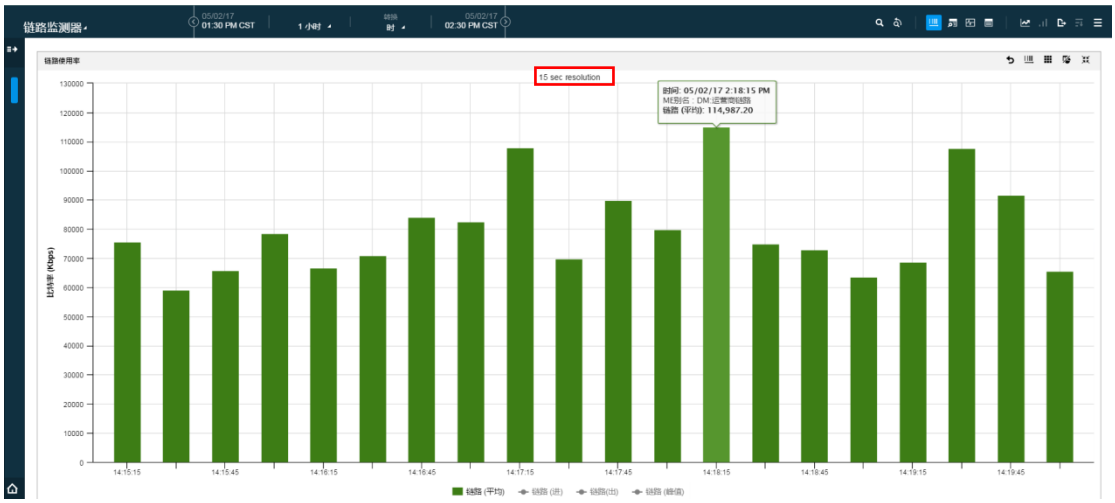
在链路监测器左下角的柱状图中，选择某一具体柱体，可查看该 5 分钟内流量信息。如下图查看下午 2:15-2:20 的流量信息。

5 分钟精度：鼠标悬停在该柱体上可以查看该柱体表示的具体信息，有时间、接口以及链路用量信息

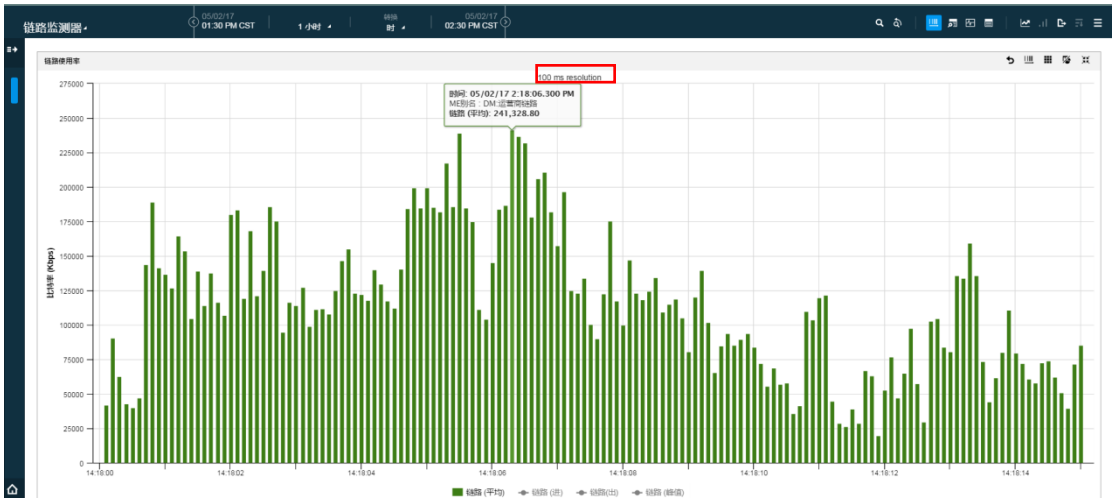


点选其中一根柱体后，点击柱状图右上方的  按钮，可以提高查看精度，如在上述 5 分钟里查看 15 秒精度的流量信息。

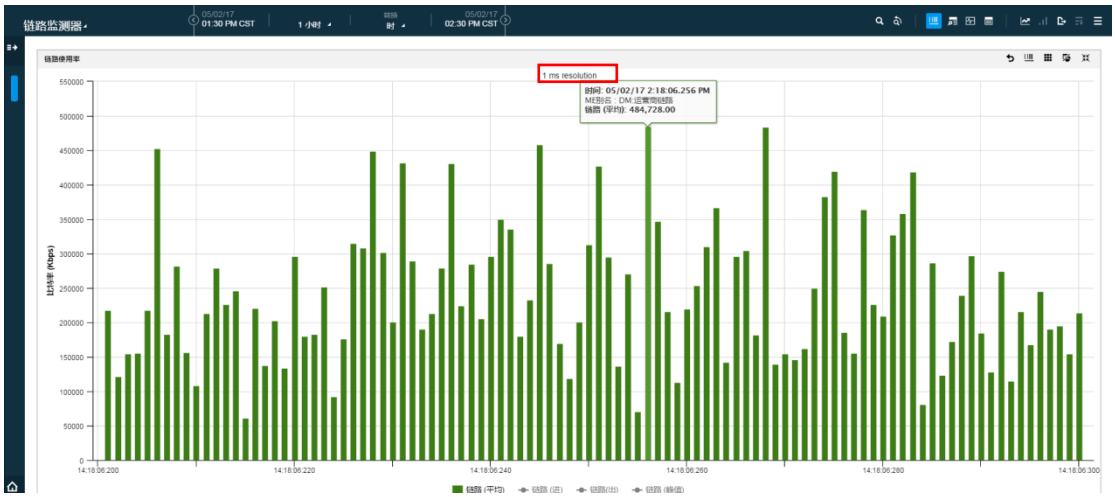
15 秒精度：能看到在下午 2:15-2:20 内，15 秒精度的流量情况



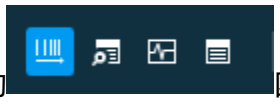
100 毫秒精度：下午 2:18:00-2:18:15 内，100 毫秒精度的流量情况



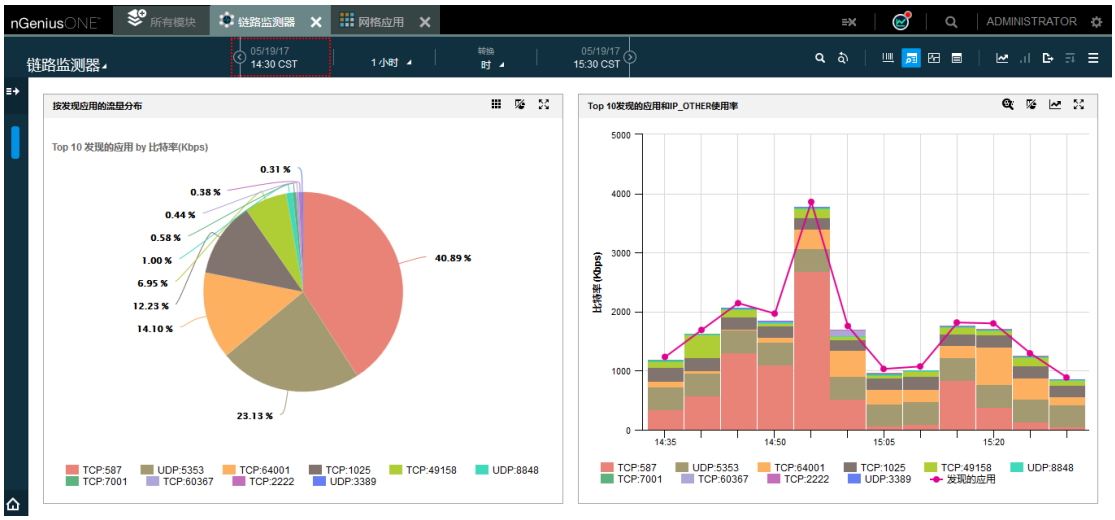
1 毫秒精度：下午 2:18:06.200-2:18:06.300 内，1 毫秒精度的流量情况



④ 链路监测器的四种模式

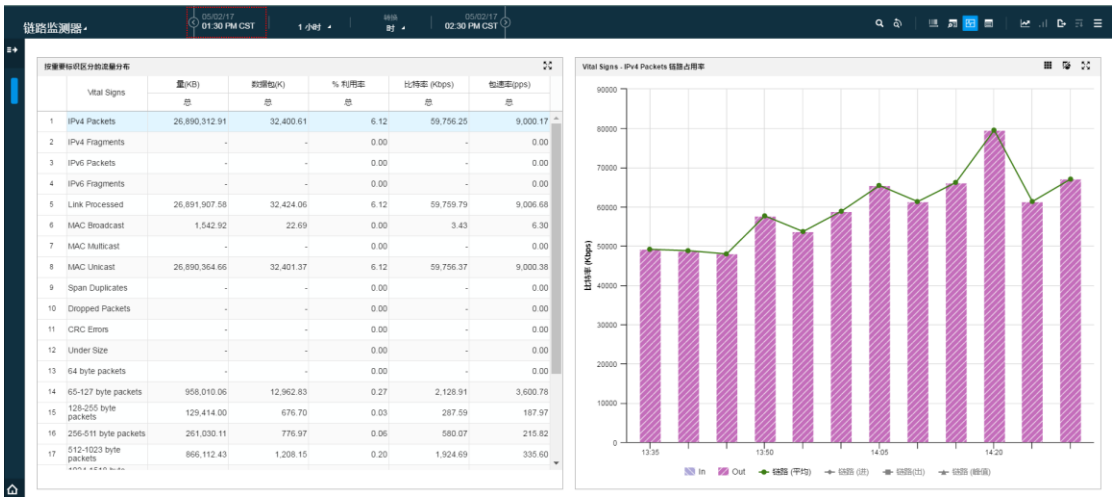
界面左上方工具栏中的  四个按钮，分别对应链路监测器的深入粒度分析模式、应用发现模式、Vital Signs 模式以及应用模式。进入链路监测器时，默认进入深入粒度分析模式，该模式上文已有介绍，这里不再累述。

在链路监控界面点击右上方的  按钮，切换至“应用发现”模式。该模式下可查看 TOP 10 的未定义应用以及这些应用的流量信息。

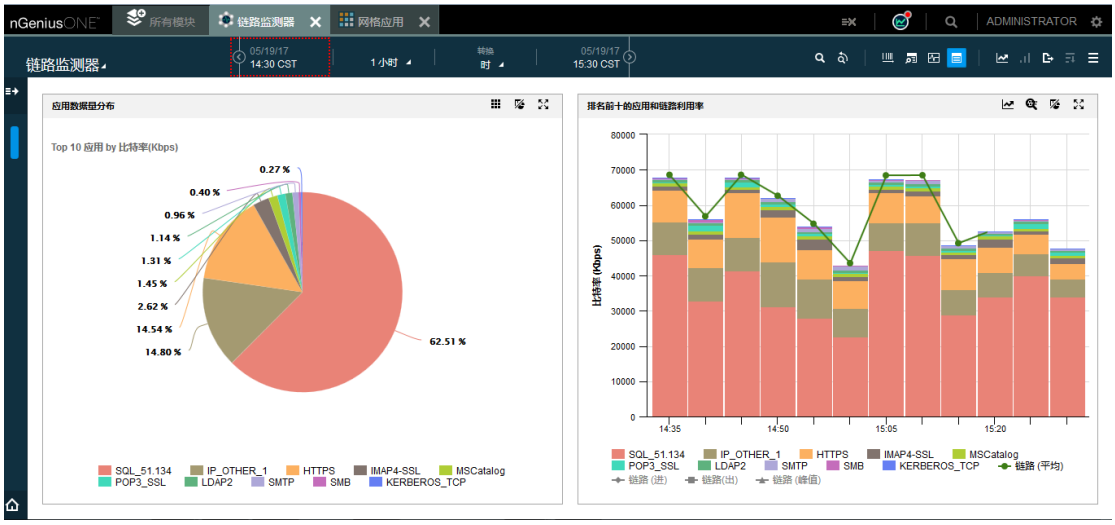


“Vital Signs”模式  。在该界面下可查看 IPv4 流量、组播流量、广播流量以及丢包情况

等流量信息。

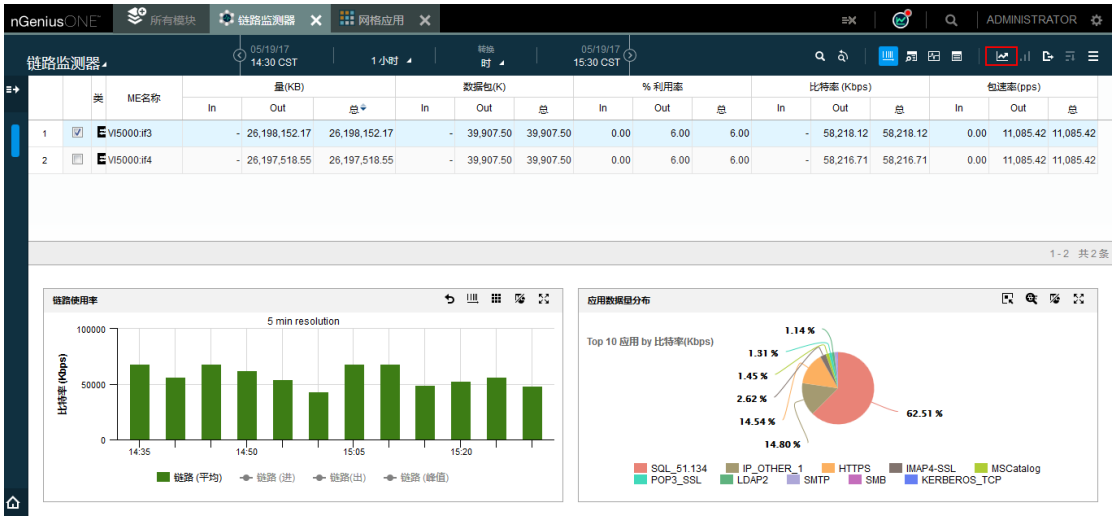


应用模式，该界面下可查看 TOP 10 通识应用以及已定义应用的在流量中的占比以及各应用的用量信息。

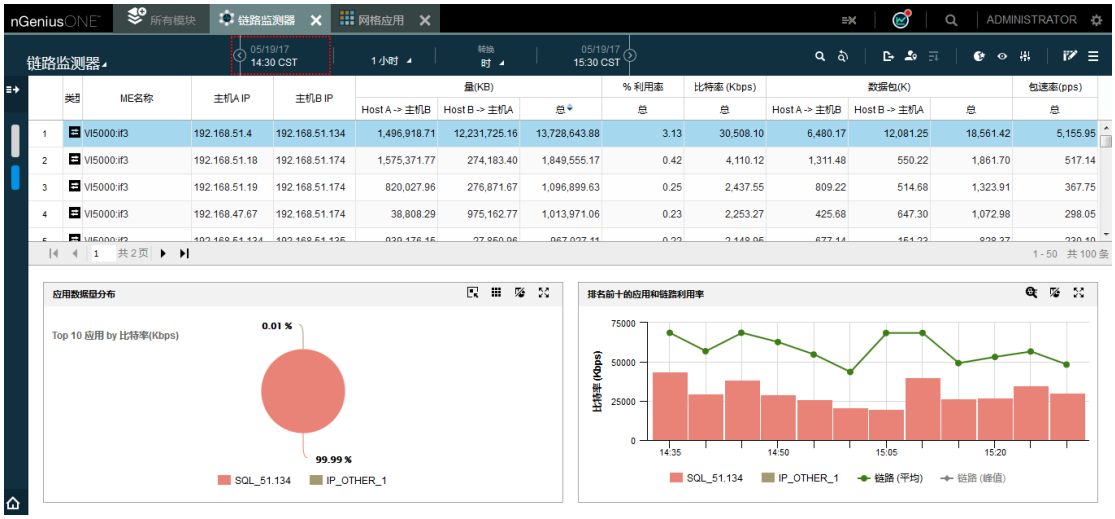


⑤ 会话视图

在链路监测器界面点击按钮，可启动会话视图。

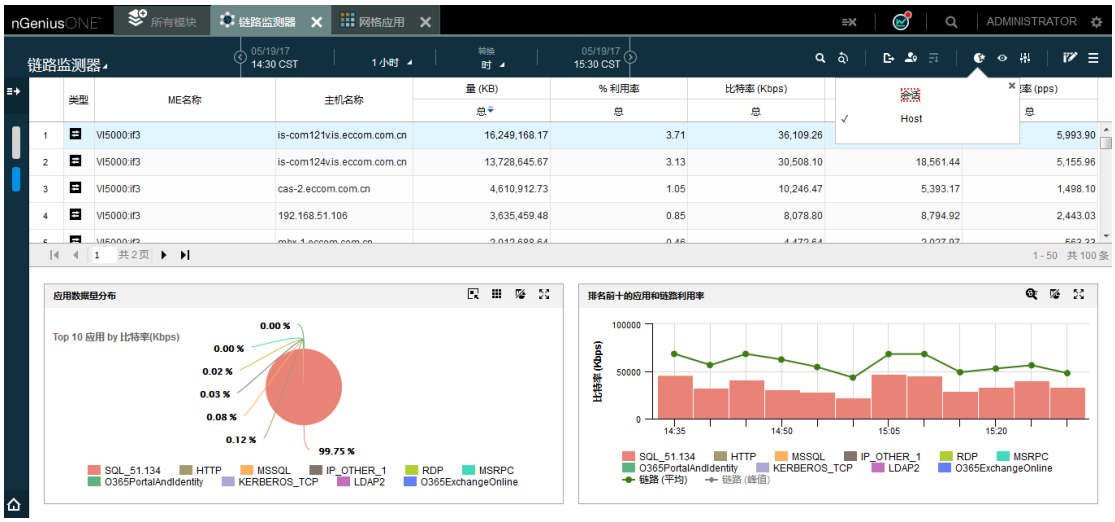


在会话视图中可查看链路内通讯对的详细信息，包括所选时间段内通讯对双向流量大小、数据包数量、包率以及应用成分信息等。

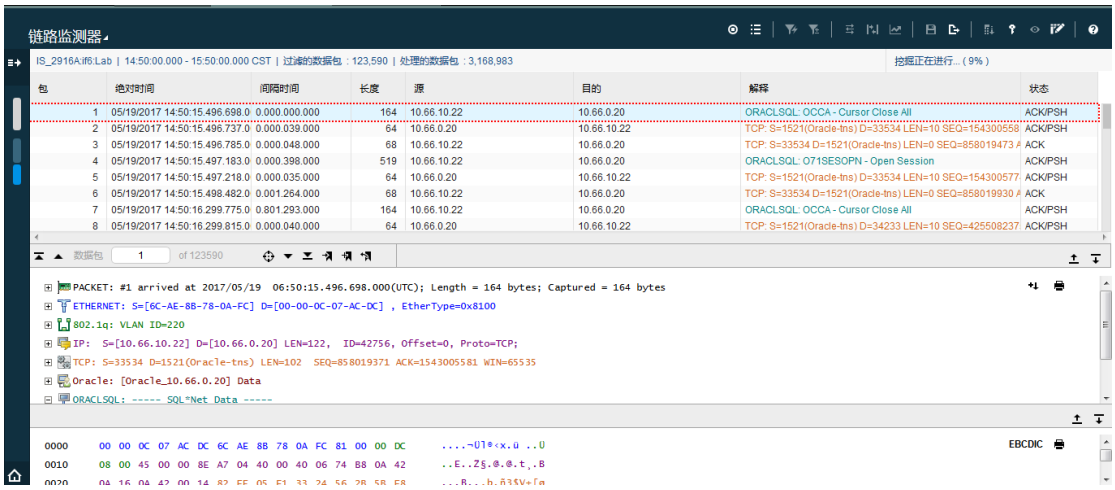


点击右上方工具栏中的  按钮，可调出通讯对双方端口、传输协议以及关联的应用等信息。

点击右上方工具栏中的  按钮，可将界面更改为展示主机用量信息。



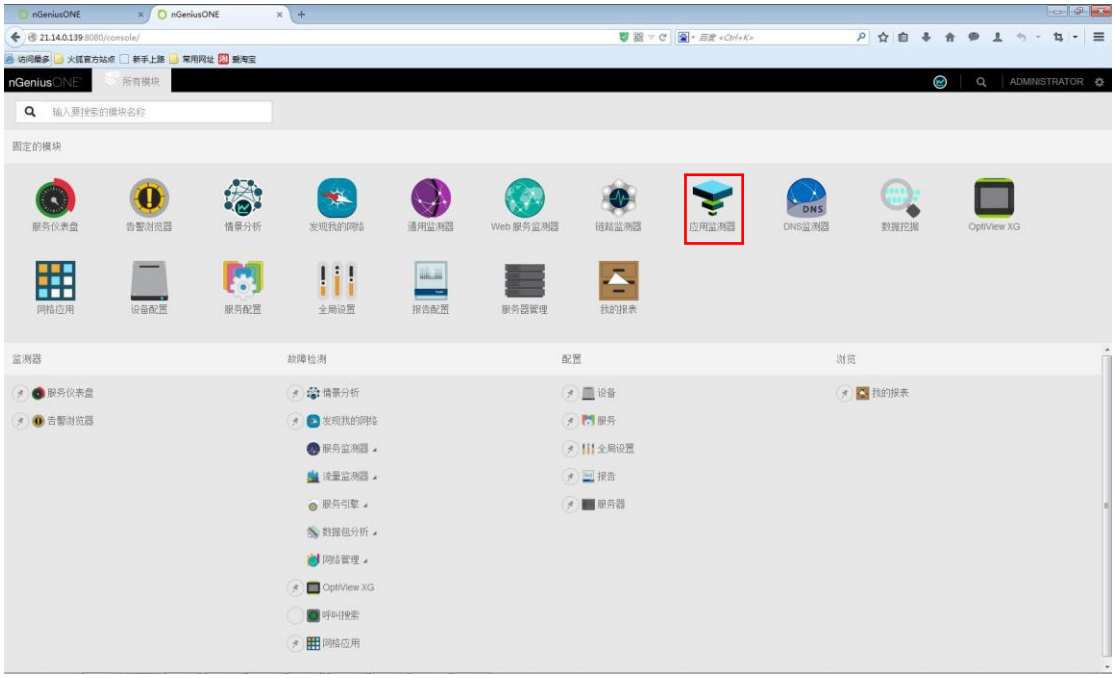
选中其中一个通讯对或主机后，点击该界面右下方的  按钮，可进入数据包解码界面，查看该通讯对或主机的数据包。



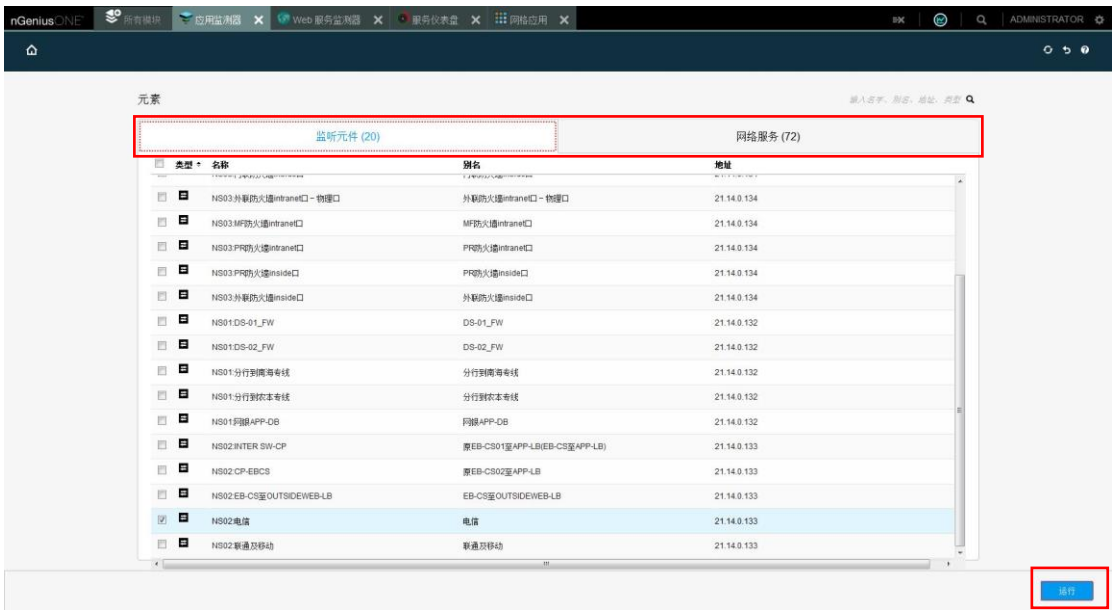
3.2.2 应用监测器

应用监测器可提供网络中的流量统计以及应用成分分析，当想要查看某条链路或者分行中包含的应用成分以及分布情况时，可以使用应用监测器查看。

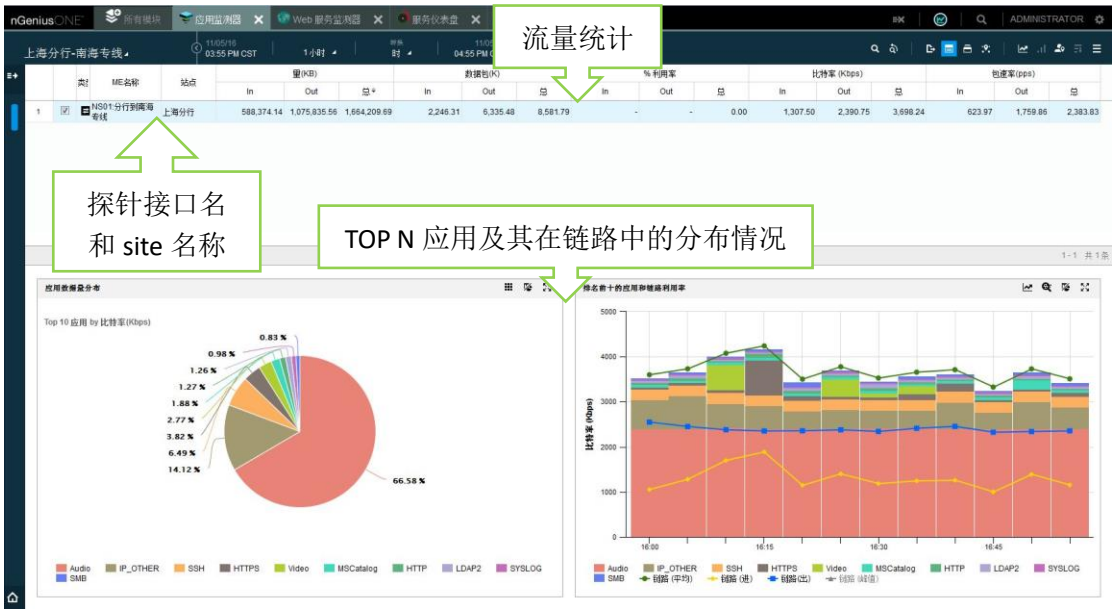
“所有模块”→“应用监测器”



进入应用监测器，选择需要查看的接口或者网络服务（同一类型可多选，在监测器界面会以多个条目的形式展示），然后点击“运行”

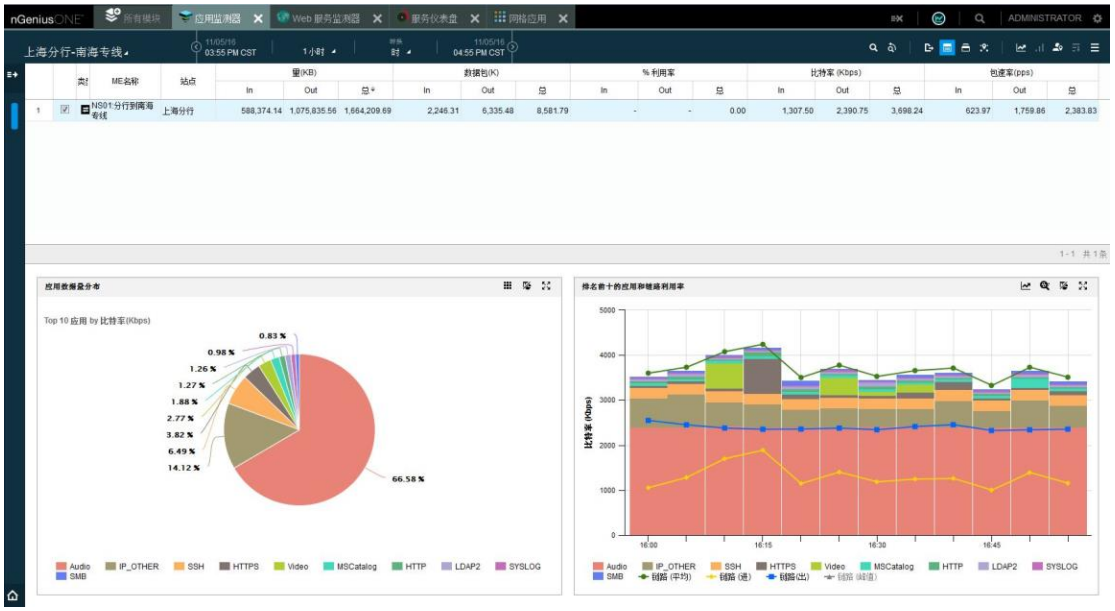


应用监测器界面分为上方表格框以及下方图表区域，表格框中列出了选定时间段内链路中的流量情况，图表区域展示了选中接口或网络服务下的 TOP N 应用及其分布情况，如图：

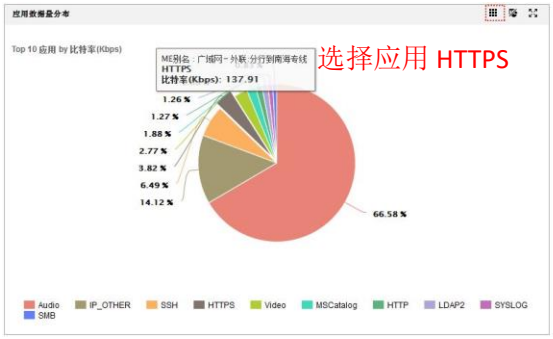


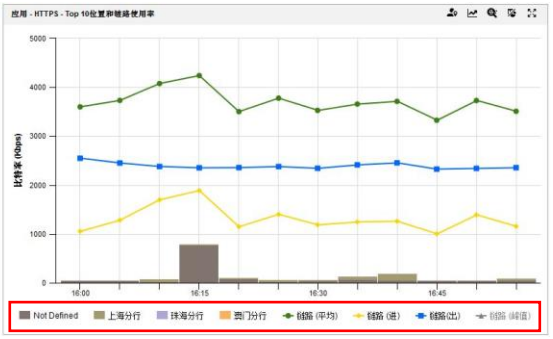
应用监测器共有三种模式，应用模式、应用组模式以及位置模式，各模式的详细介绍如下：

① 应用模式（与链路监测器中的应用模式类似）

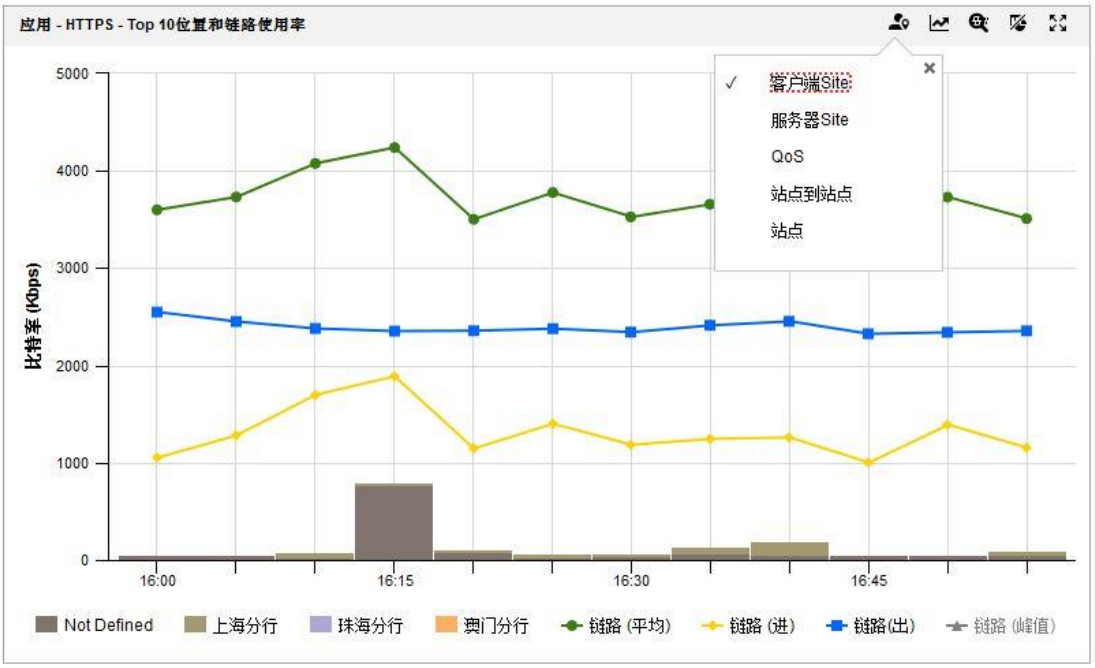


当我们选择左下方饼图中的某个应用时，能够查看到该应用在分行 site 中的分布情况



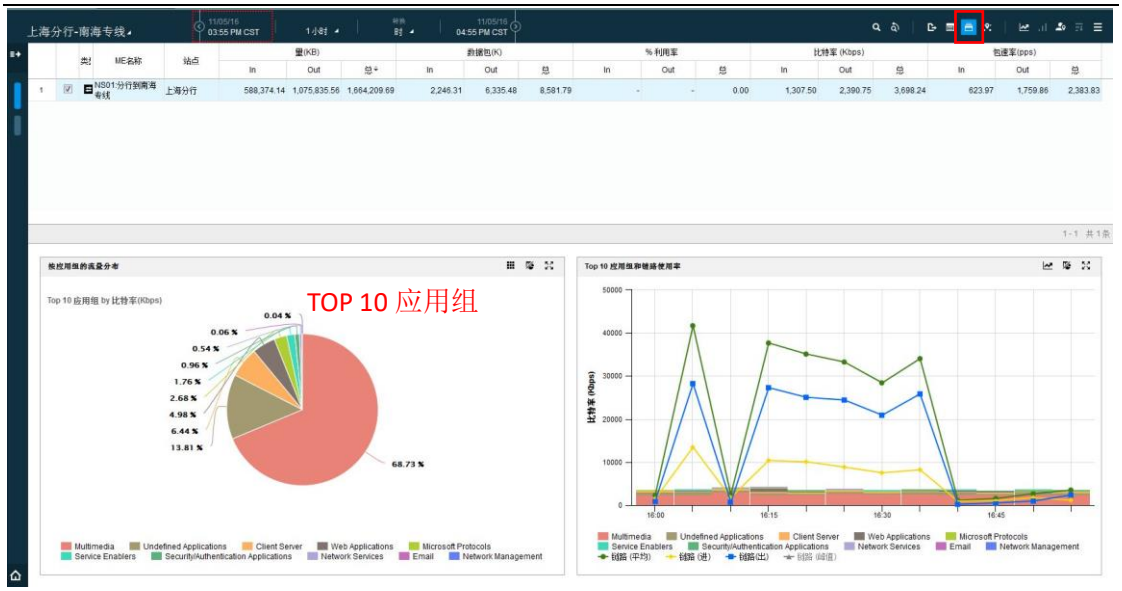


查看对象有“客户端 site”、“服务器 site”、“QoS”、“站点到站点”、“站点”几种

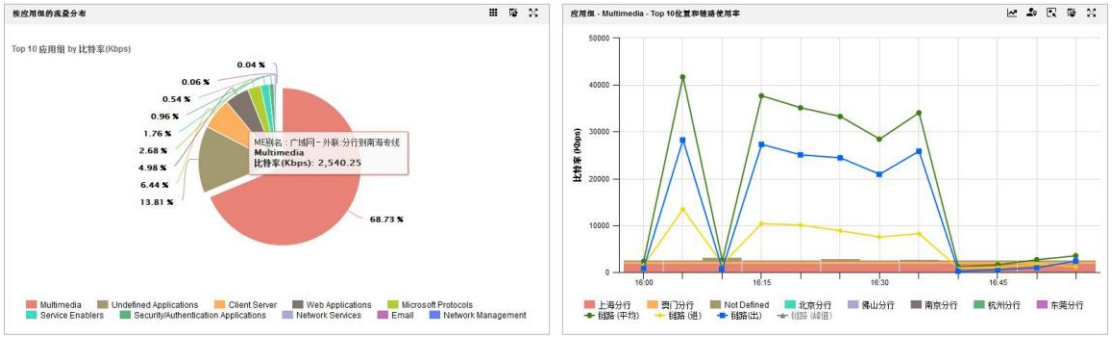


② 应用组模式

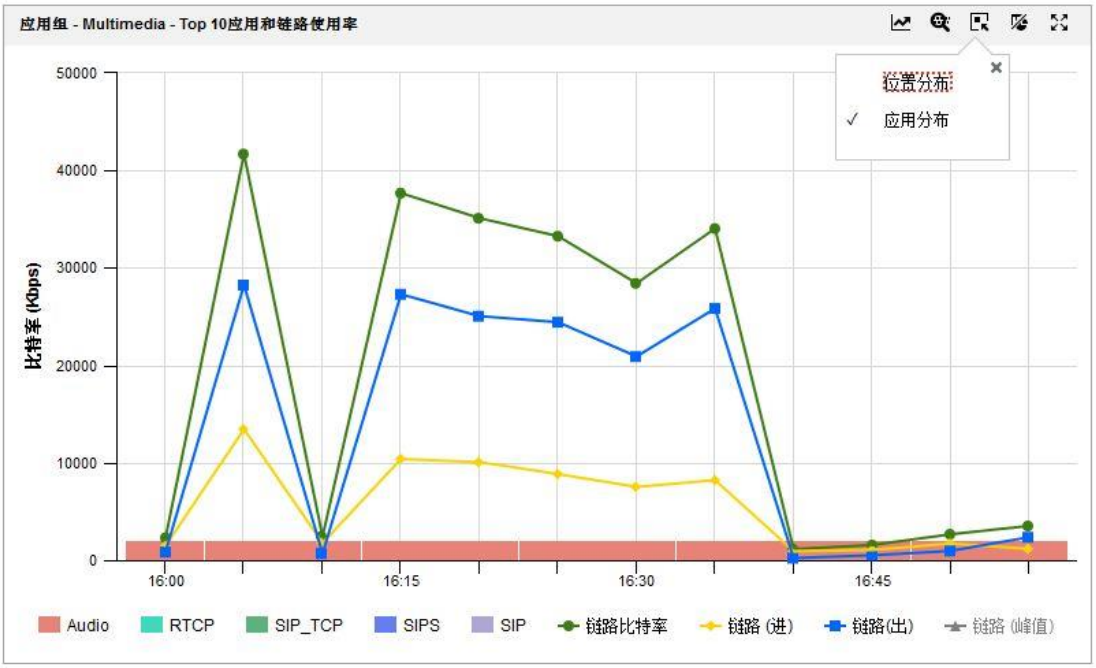
点击界面右上方  图标可将监测器切换至应用组模式，此时界面展示的是各个应用组在接口下的流量情况以及分布情况



同样可以选择单一应用组来查看应用组流量在分行 site 的分布情况

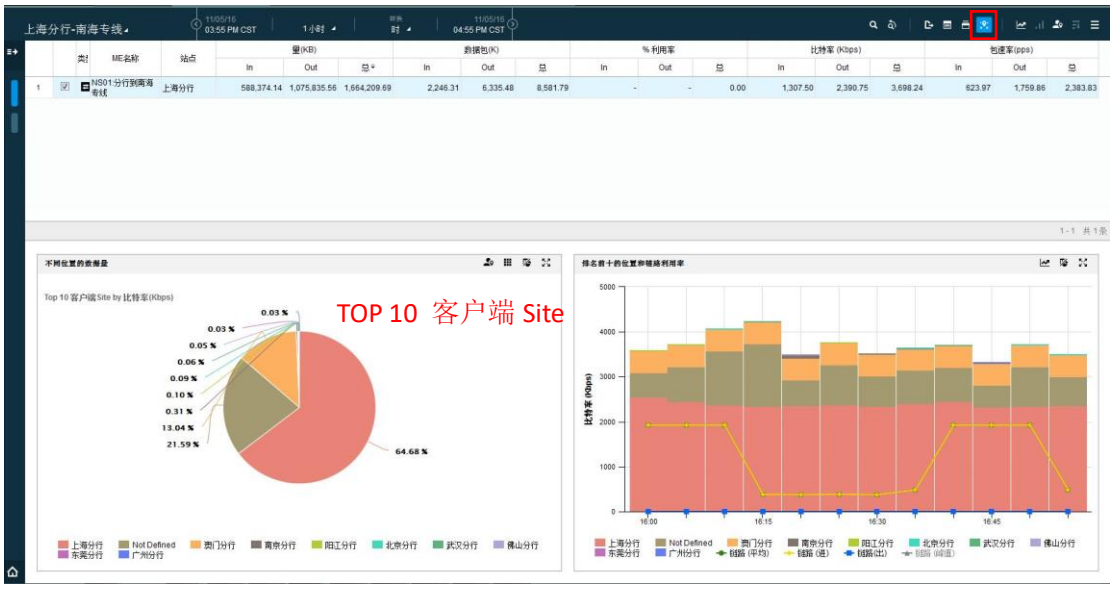


或点击柱状图右上方的  后选择“应用分布”来查看应用组内各应用的分布情况

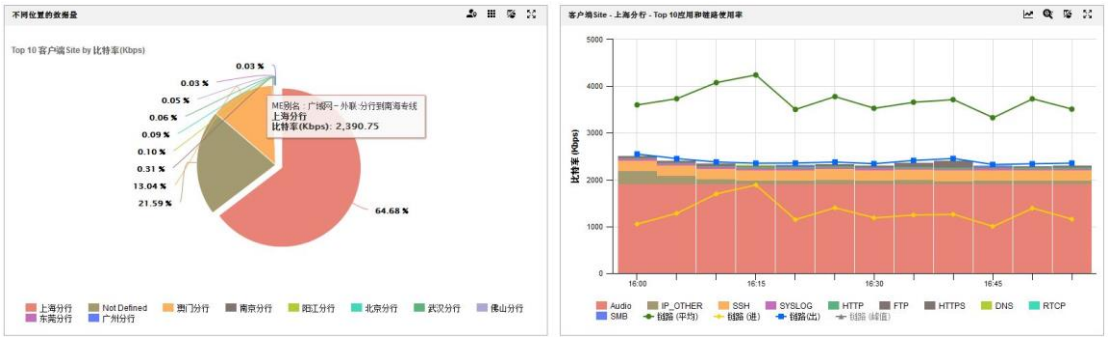


③ 位置模式

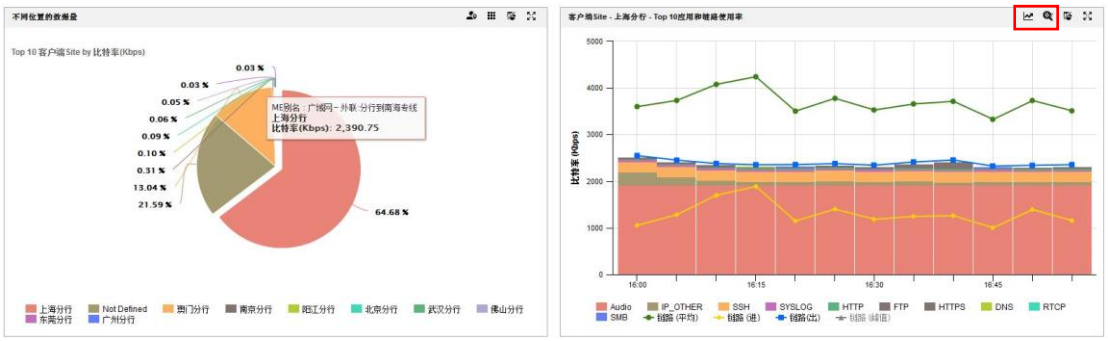
点击界面右上方  图标可将监测器切换至位置模式，该模式下监测的是 TOP 10 客户端 site 的流量分布



点选单个客户端 site，右边的柱状图则会统计出 site 间的 TOP 10 应用流量分布



在三个模式下，我们都可以点击  和  来进入会话视图以及数据包解码界面



3.3 服务监测器

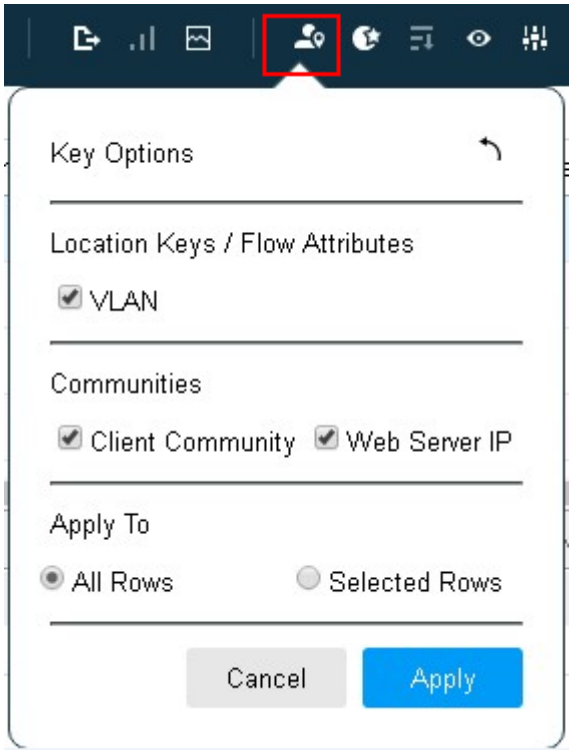
nGeniusONE 有多种监测器，针对用户网络中的不同应用服务，协助运维人员更有针对性地进行排障。

3.2.1 Web 服务监测器

Web Services 监测器可以给在“应用”的“HTTP”类别下定义的 HTTP 应用和基于 URL 以及服务器的应用程序进行深入的追踪并提供详细的性能指标。在监测器上部表格窗体中可以查看该 WEB 应用各参数（Get、Head、PutPost、Others）的延迟、请求、错误等数据。在下方图表窗体中可以查看对应的延迟、利用率、交易量、应用错误编码等信息的时间分布情况。

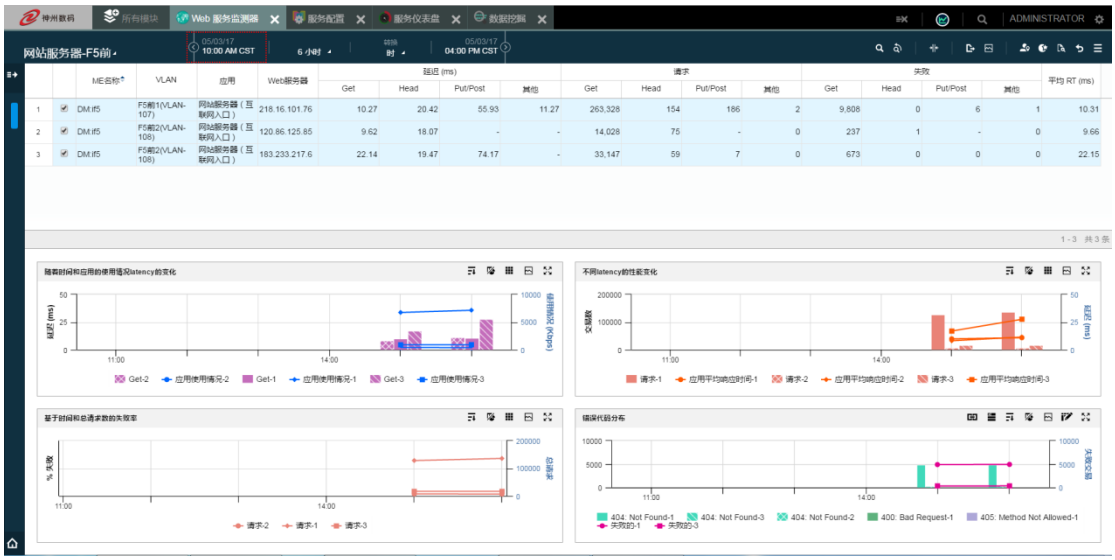
Web 服务监测器中可展现的参数如下：

点击工具栏的  按钮可以对表格显示的项目进行更改，增加 VLAN 号信息。



当需要将多个服务器的情况进行对比时，可以同时勾选多行，然后点击工具栏中的  按钮来进行对比查看。如下图，下半部的图表中将 218.16.101.76、120.86.125.85 和

183.233.217.6 三台服务器聚合展示。



3.2.2 数据库监测器

在监测器上部表格窗体中可以查看该数据库各项操作（Connect、Query、Modification、others）的延迟、请求、错误等数据。在下方图表窗体中可以查看对应的延迟、利用率、交易量、应用错误编码等信息的时间分布情况。

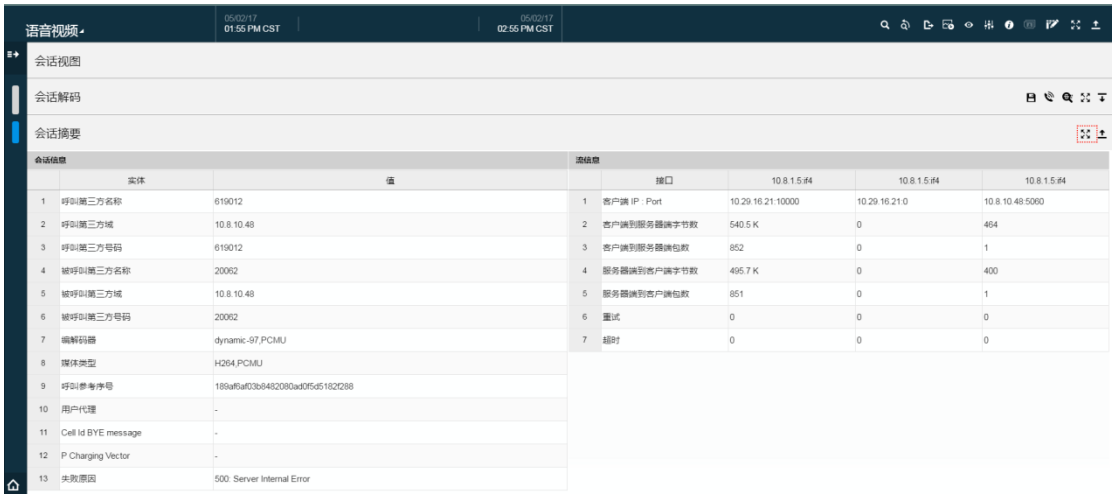
数据库监测器中可展现的参数如下：

3.2.3 呼叫服务监测器

在呼叫服务监测器中可看到呼叫的请求数、失败数、延迟、呼叫建立、拆除等信息

呼叫服务监测器中可展现的参数如下：

点击监测器界面的  按钮，下钻到会话视图查看单个呼叫的详细信息，包括呼叫双方号码、重传、延时、持续时长等

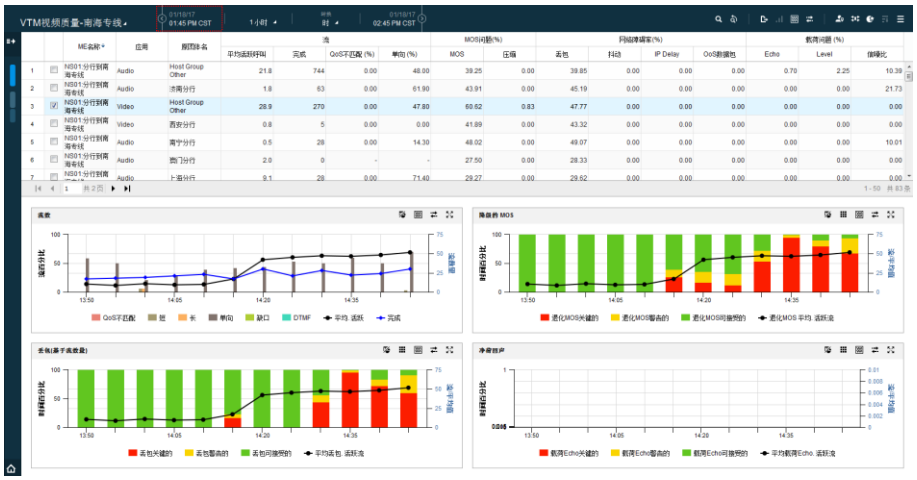


	实体	值
1	呼叫第三方名称	619012
2	呼叫第三方域	10.8.10.48
3	呼叫第三方号码	619012
4	被呼叫第三方名称	20062
5	被呼叫第三方域	10.8.10.48
6	被呼叫第三方号码	20062
7	编解码器	dynamic-97,PCMU
8	媒体类型	H264,PCMU
9	呼叫参考序号	189af6af03b8482080ad0f5d5182f288
10	用户代理	-
11	Cell Id BYE message	-
12	P Charging Vector	-
13	失败原因	500: Server Internal Error

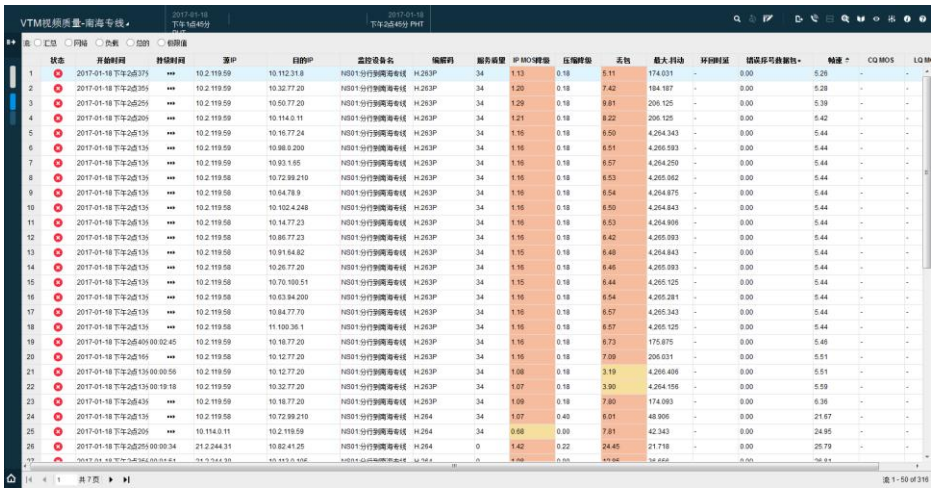
	接口	10.8.1.5:if4	10.8.1.5:if4	10.8.1.5:if4
1	客户端 IP : Port	10.29.16.21:10000	10.29.16.21:0	10.8.10.48:5060
2	客户端到服务器端字节数	540.5 K	0	464
3	客户端到服务器端包数	852	0	1
4	服务器端到客户端字节数	495.7 K	0	400
5	服务器端到客户端包数	851	0	1
6	重试	0	0	0
7	超时	0	0	0

3.2.4 媒体监测器

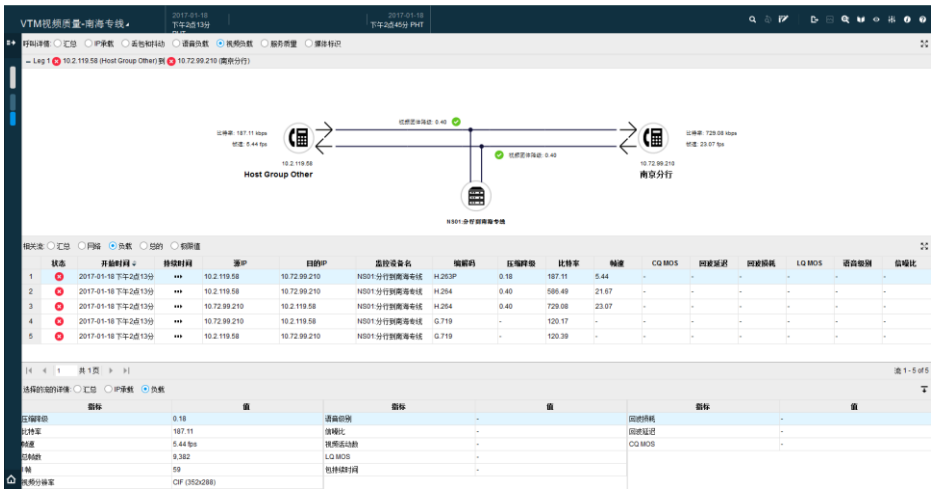
在媒体监测器中可查看视频应用分析概况，包括流统计、MOS 问题、网络障碍率、载荷问题等情况



下钻至流视图，查看各个视频流的信息，包括视频压缩技术、帧率、比特率等



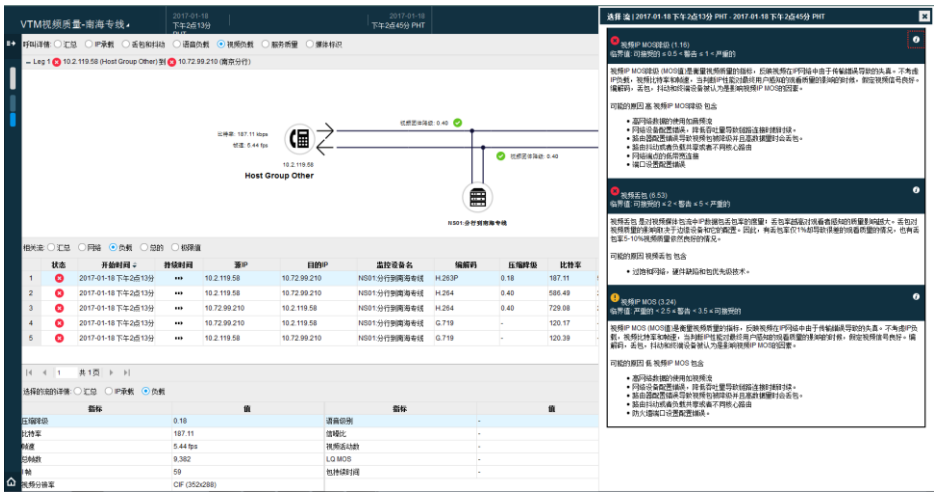
下钻到单个呼叫视图，对单个呼叫进行分析，查看视频编码的性能和错误、视频应用载荷应用行为等信息



选择的流的详情: ◯ 汇总 ◯ IP承载 ◉ 负载

指标	值
压缩降级	0.18
比特率	187.11
帧速	5.44 fps
总帧数	9,382
I 帧	59
视频分辨率	CIF (352x288)

结果助手：对当前视频指标值评级并给出可能的原因供用户参考



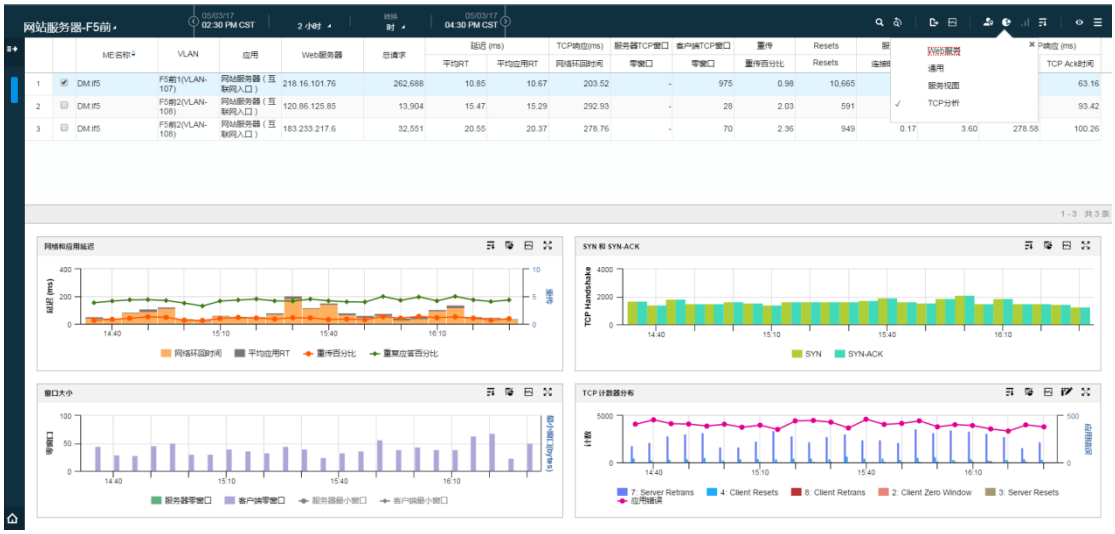
3.2.5 通用监测器

对于非通识应用，我们可以使用通用监测器查看其应用情况。在通用监测器界面中可以看到网站服务器这一应用的总请求数、总延迟、应用延迟、TCP RTT、重传数等指标。

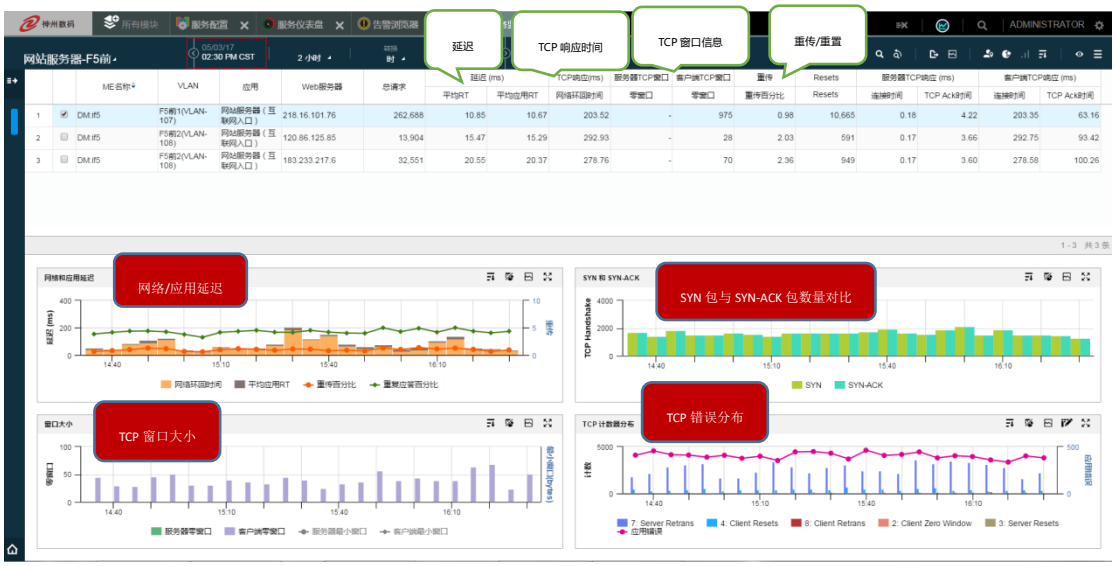
通用监测器中可展现的参数如下：

3.2.6 TCP 分析

在应用监测器 (以 Web 服务监测器为例) 的工具栏中点击  按钮可以切换至 “TCP 分析” 视图



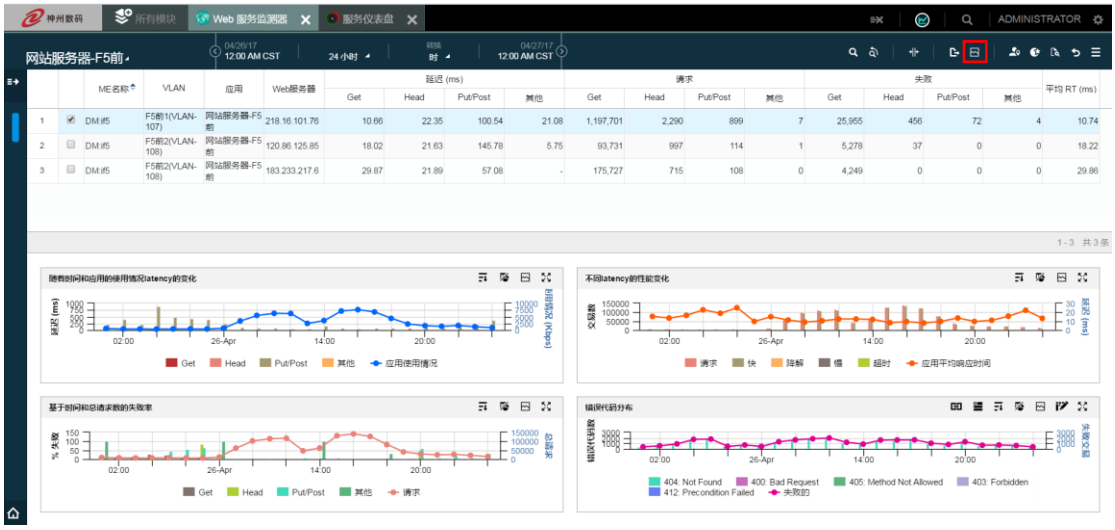
TCP 分析界面中，在上部表格窗体中可以查看该 TCP 应用的总延迟和应用延迟、TCP 平均响应时间、服务器 TCP 0 窗口事件、客户端 TCP 0 窗口事件、TCP 重传、重置等信息。下方图表窗体中可以查看响应时间、SYN/SYN-ACK 数量、TCP 0 窗口和小窗口事件等信息的时间分布情况。



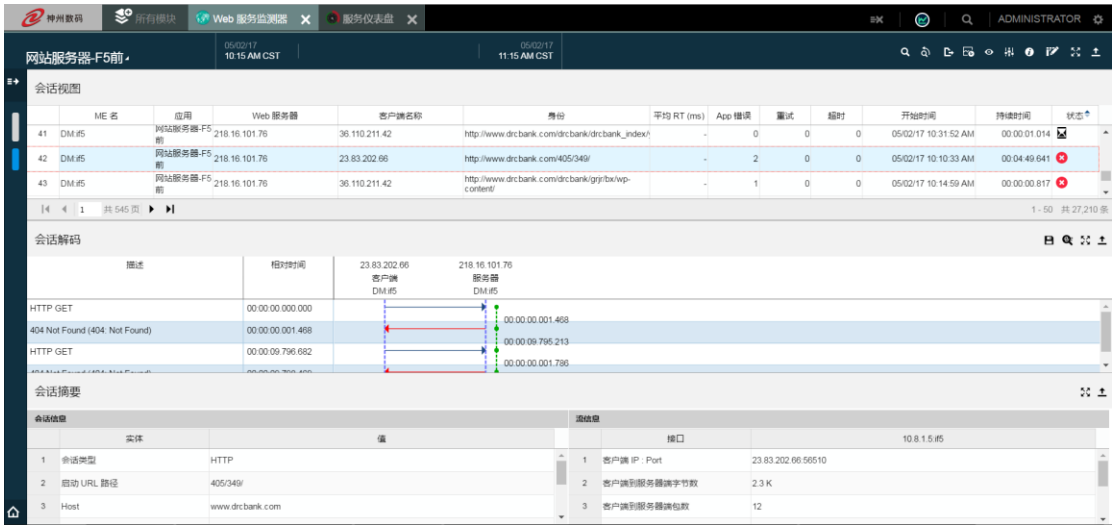
3.2.7 会话分析

如果想对应用进行更深层的分析，可在相应应用监测器的工具栏点击按钮，进入会话分析界面。

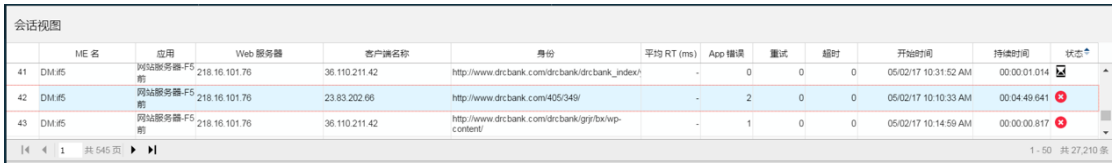
如从 Web 监测器界面中进入会话分析界面。



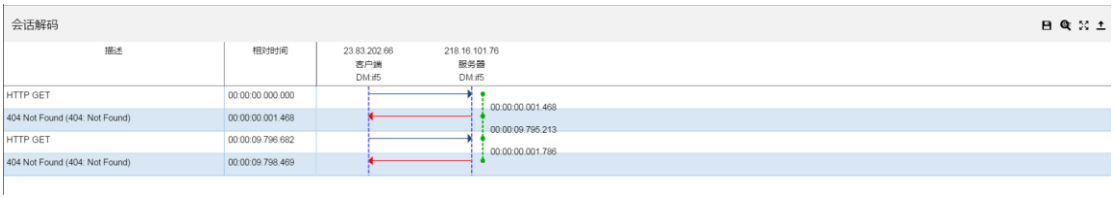
会话分析界面分为三部分，分别为：会话视图、会话解码、会话摘要：



会话视图，能看到选定时间段内所有会话的概要信息，如通信对地址、平均延时、应用错误数量、重传数、超时数、会话开始时间、会话持续时间等信息。

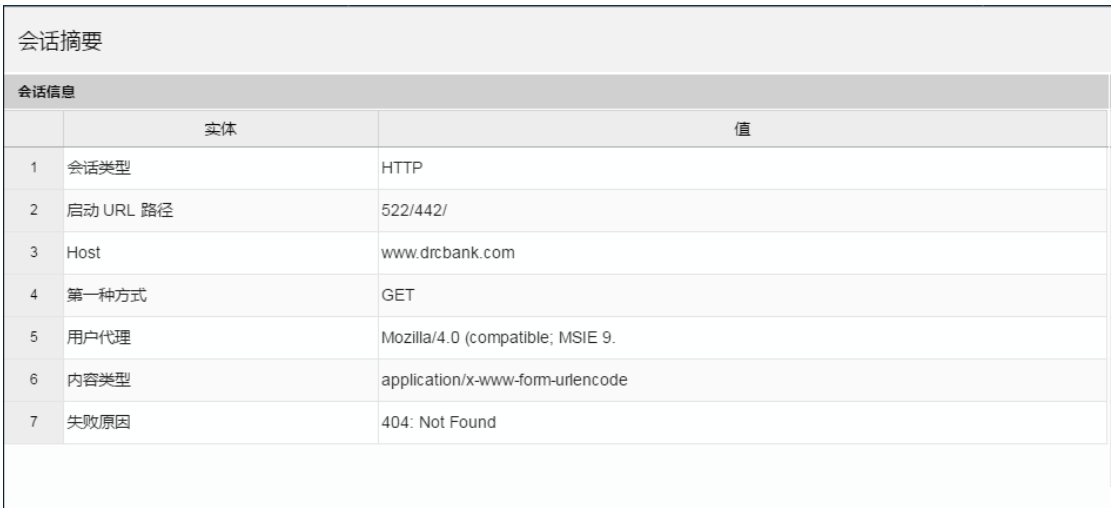


会话解码，跟踪选中会话的通信过程，有对传输数据的简单描述；在出现应用错误处会用红色箭头显示，表示出错；在相对时间中也能看到通信过程中的延时信息。



会话摘要，包括会话信息和流信息：

会话信息，可看到会话的详细信息，如在 HTTP 应用中可以查看用户代理、动作、错误代码等信息。



会话摘要

会话信息

	实体	值
1	会话类型	HTTP
2	启动 URL 路径	522/442/
3	Host	www.drcbank.com
4	第一种方式	GET
5	用户代理	Mozilla/4.0 (compatible; MSIE 9.
6	内容类型	application/x-www-form-urlencode
7	失败原因	404: Not Found

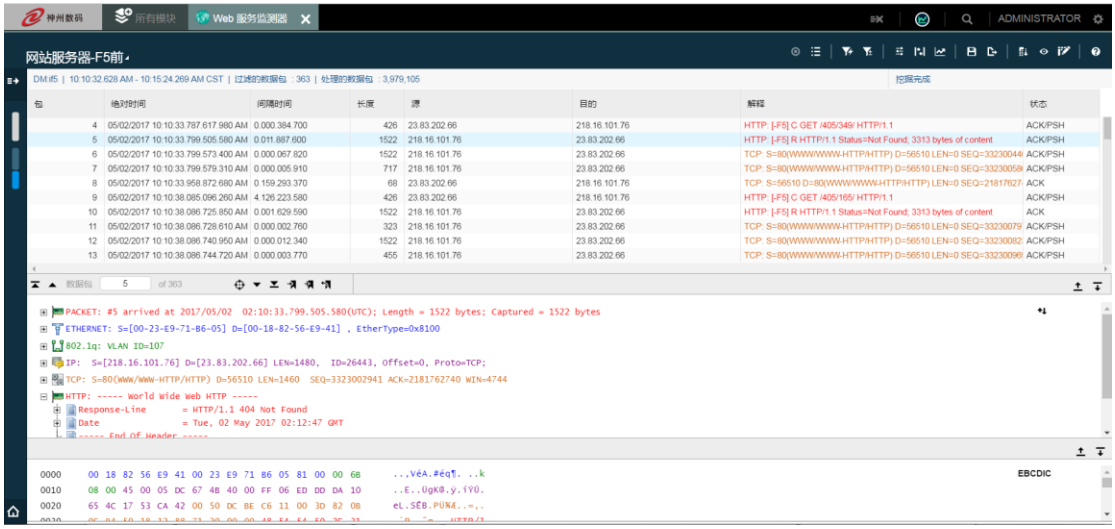
流信息，查看部分流量信息，如端口、重传数、TCP 标识等信息。

流信息

	接口	10.8.1.5:if5
1	客户端 IP：Port	23.83.202.66:63238
2	服务器 ACK 时间 (ms)	8
3	客户端 ACK 时间 (ms)	70
4	服务器重复 ACK	0
5	客户端重复 ACK	14
6	服务器窗口扩展因子	0
7	客户端窗口扩展因子	3
8	TCP标识	Server Retrans

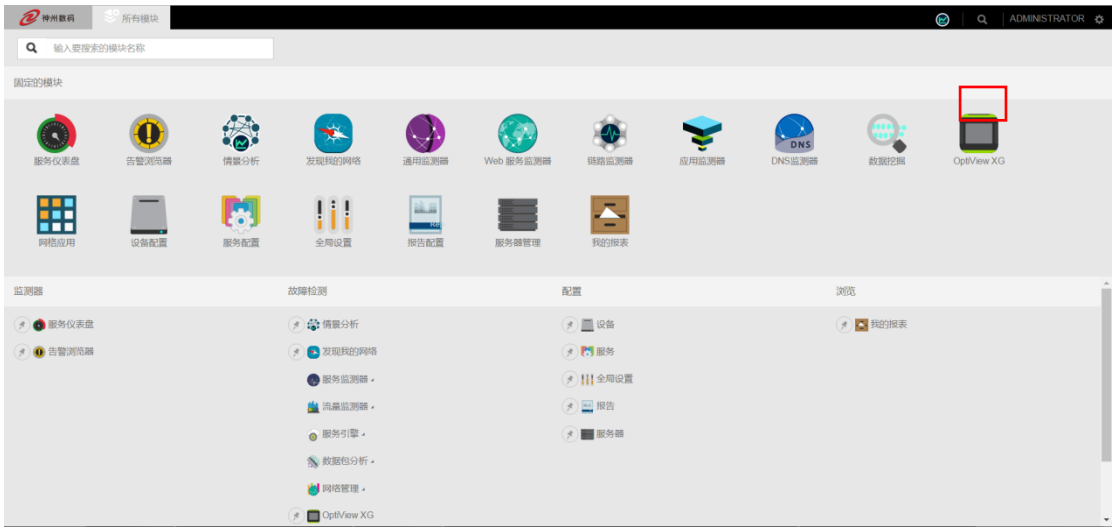
在会话解码部分，点击服务器地址或客户端地址可进入数据包解码界面。

数据包解码界面能够看到探针捕获的原始数据包。



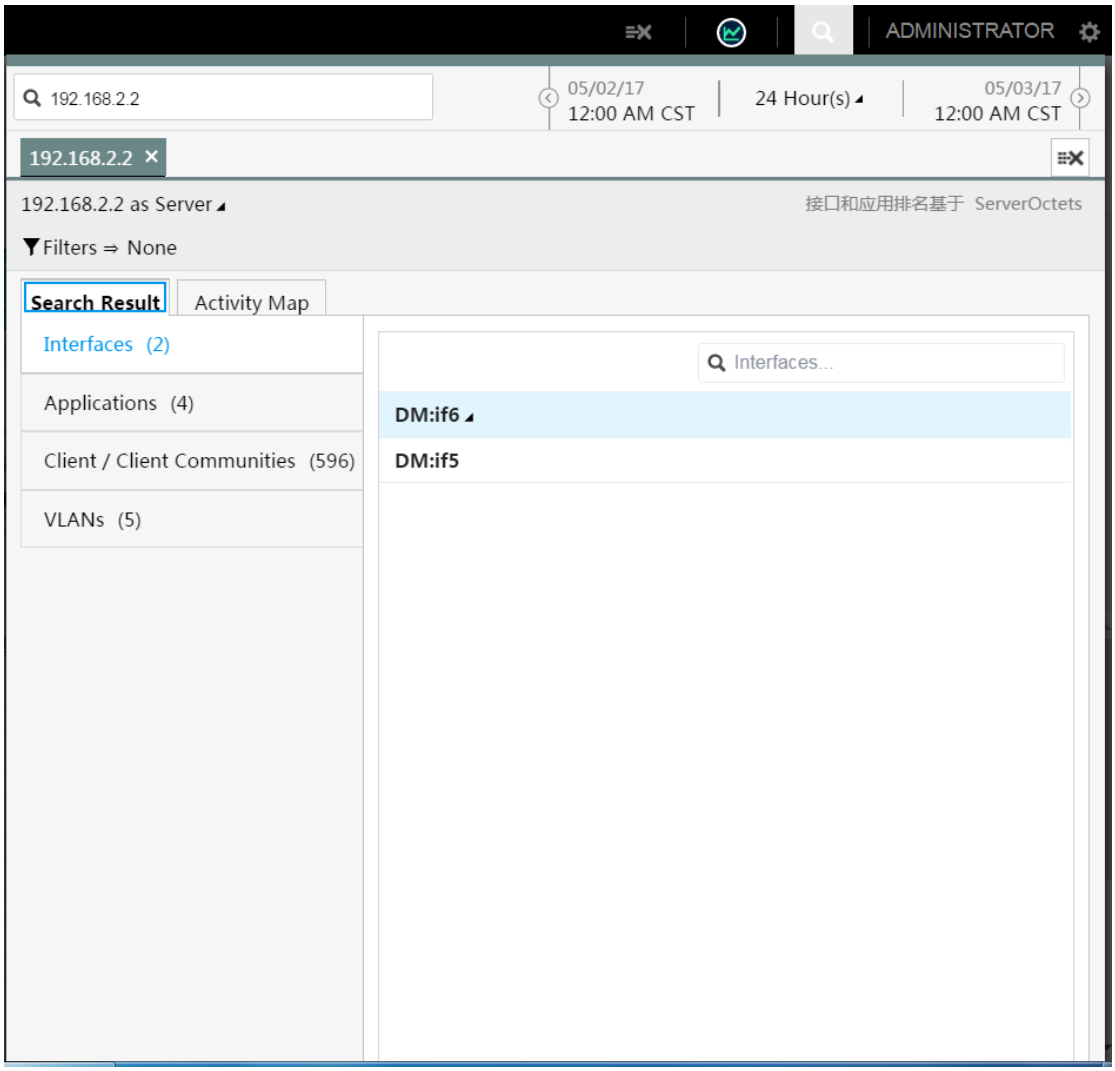
3.4 全局搜索

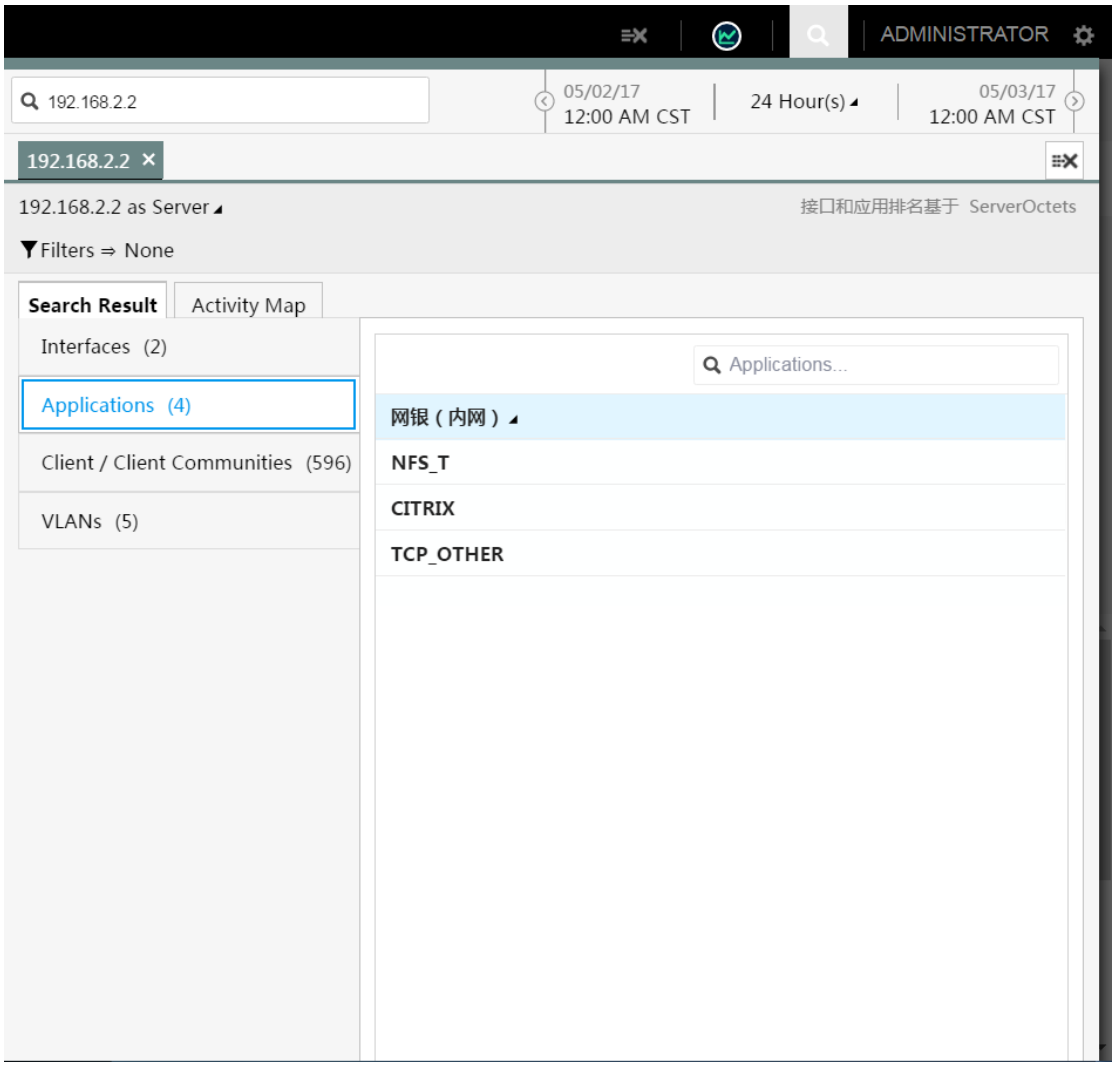
当不了解指定协议、指定 IP 或指定通讯对在哪个探针接口下时，可使用全局搜索功能进行搜索；选择 nGeniusONE 界面右上方的图标  来打开全局搜索界面；

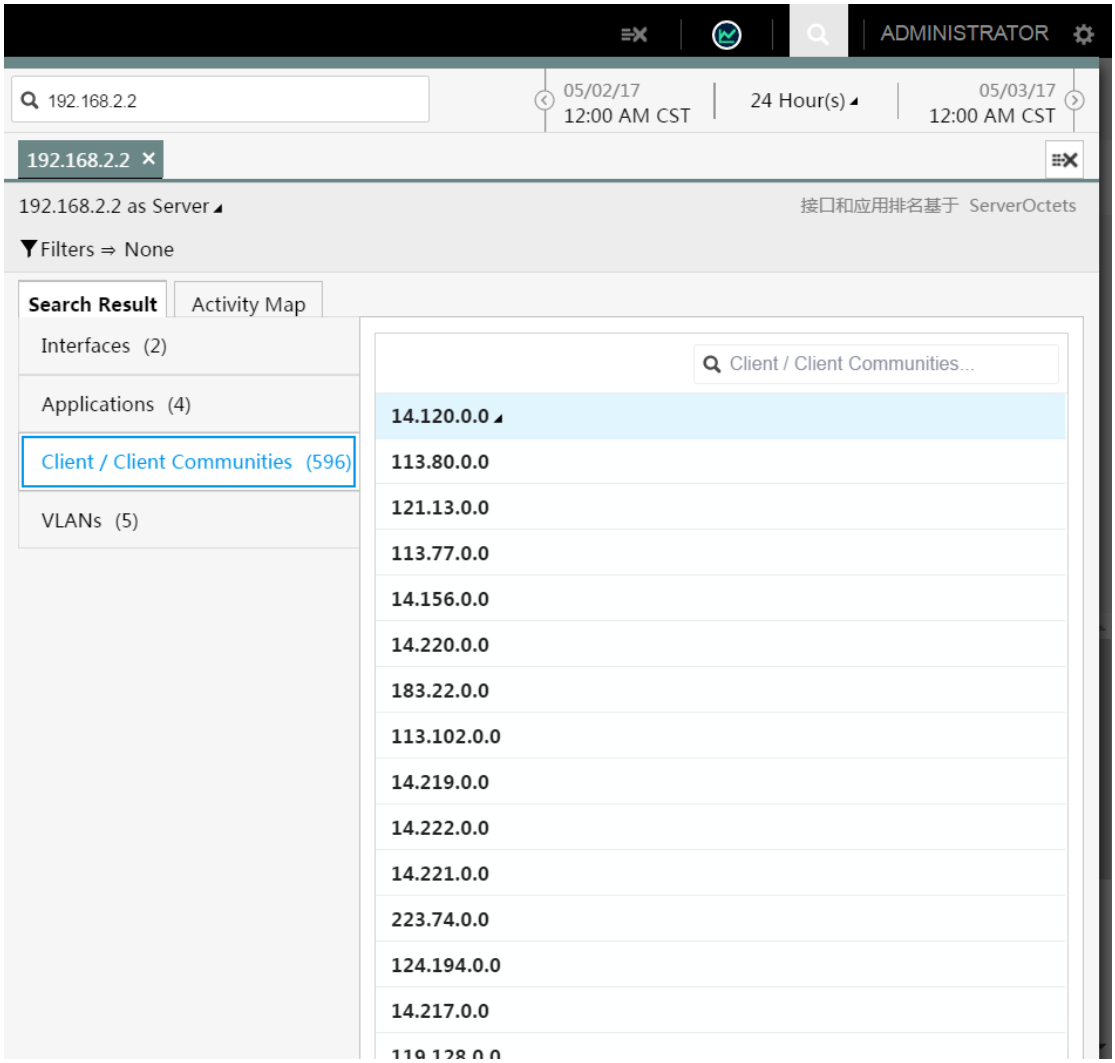


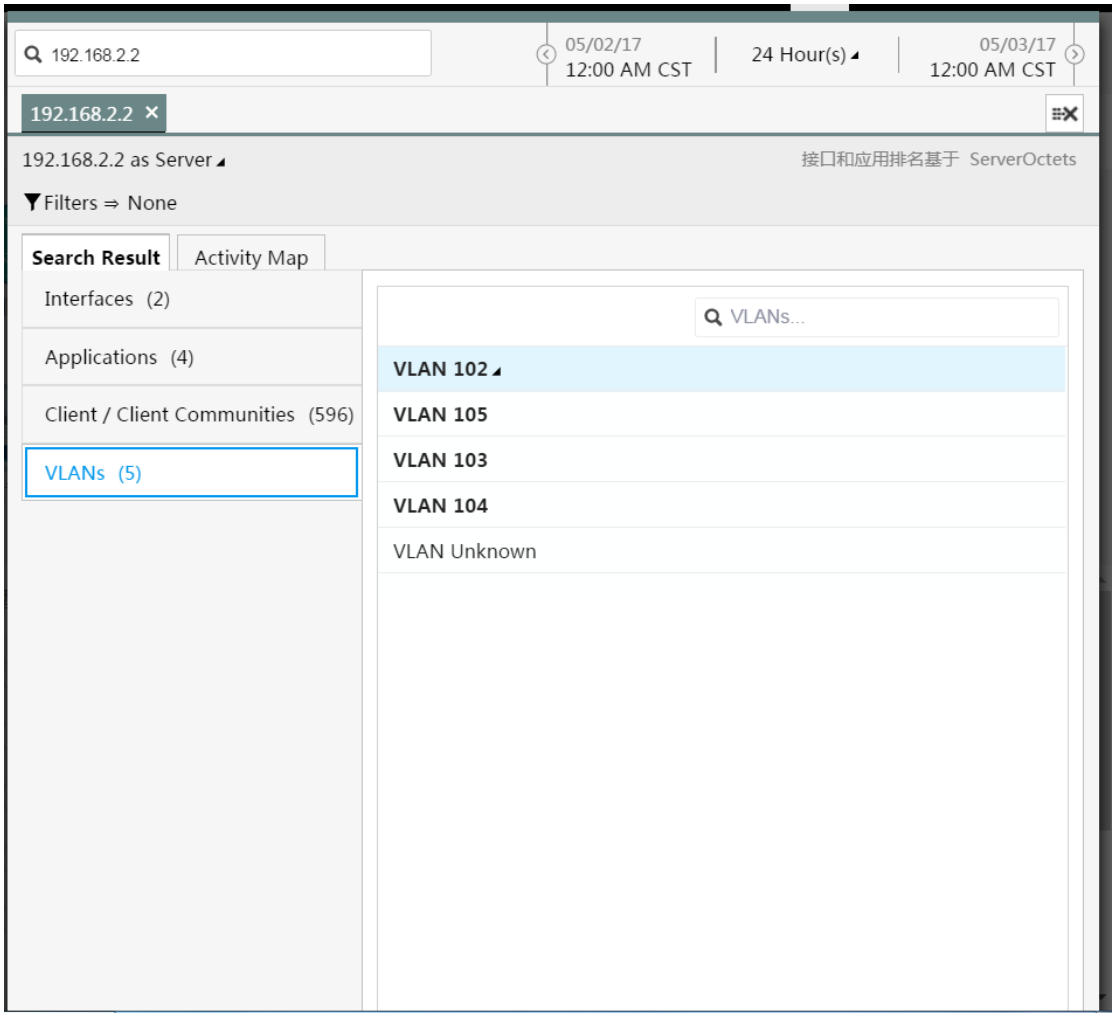
3.4.1 主机搜索

输入 IP 地址查询，能够搜索到该 IP 地址所在的探针接口，应用以及该 IP 地址作为服务器时对应的客户端；

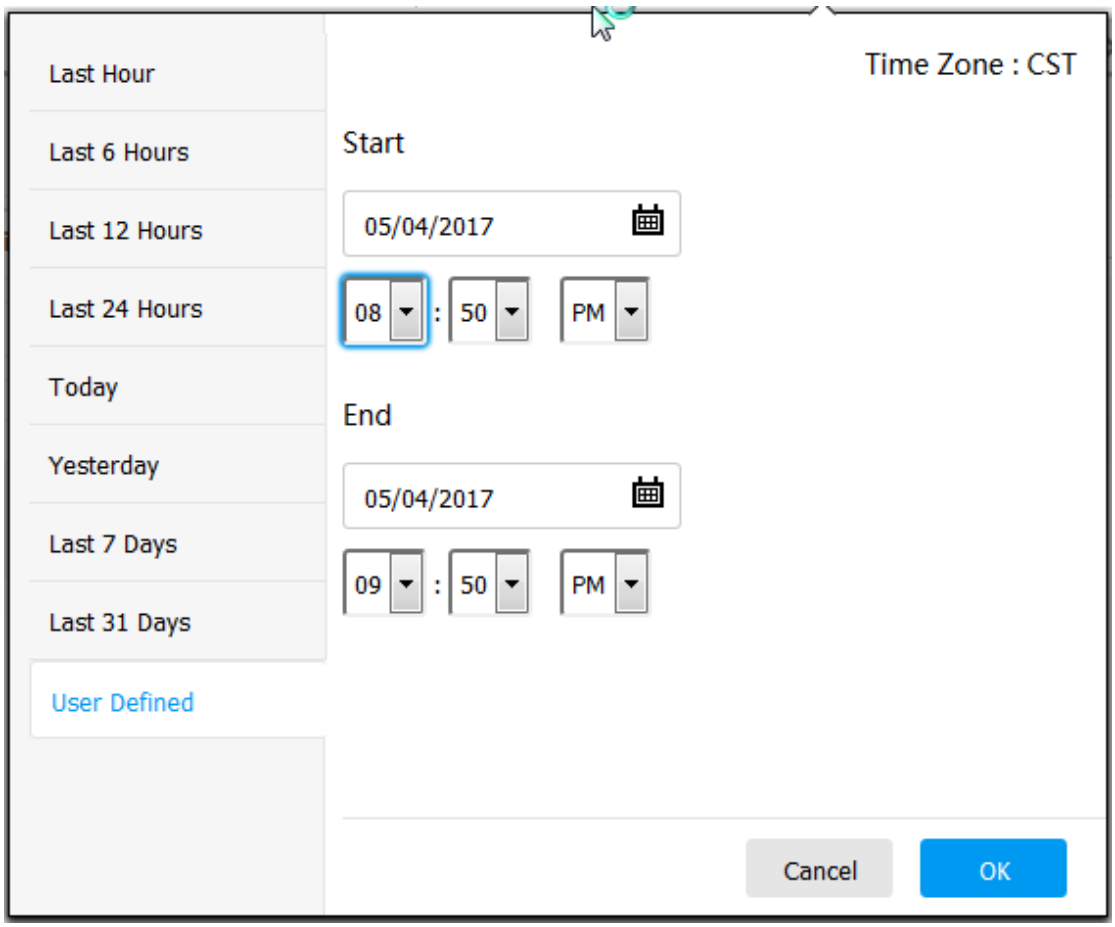

ADMINISTRATOR
192.168.2.2
05/02/17
12:00 AM CST
24 Hour(s)
05/03/17
12:00 AM CST
192.168.2.2
192.168.2.2 as Server
接口和应用排名基于 ServerOctets
Filters ⇒ None
Search Result
Activity Map
Interfaces (2)
Applications (4)
Client / Client Communities (596)
VLANs (5)
Interfaces...
DM:if6
DM:if5


ADMINISTRATOR
192.168.2.2
05/02/17
12:00 AM CST
24 Hour(s)
05/03/17
12:00 AM CST
192.168.2.2
192.168.2.2 as Server
接口和应用排名基于 ServerOctets
Filters ⇒ None
Search Result
Activity Map
Interfaces (2)
Applications (4)
Client / Client Communities (596)
VLANs (5)
Applications...
网银 (内网)
NFS_T
CITRIX
TCP_OTHER

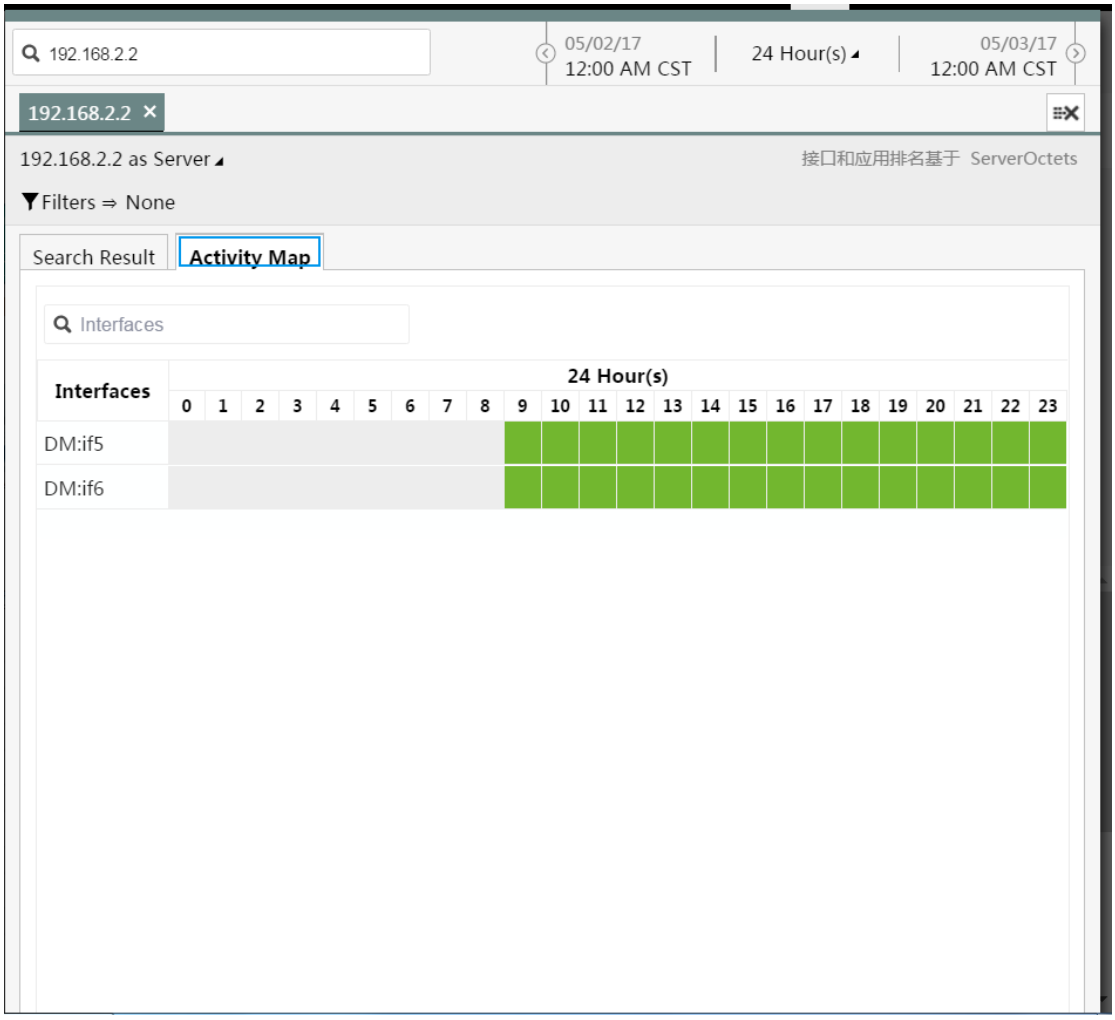

ADMINISTRATOR
192.168.2.2
05/02/17
12:00 AM CST
24 Hour(s)
05/03/17
12:00 AM CST
192.168.2.2
192.168.2.2 as Server
接口和应用排名基于 ServerOctets
Filters ⇒ None
Search Result
Activity Map
Interfaces (2)
Applications (4)
Client / Client Communities (596)
VLANs (5)
Client / Client Communities...
14.120.0.0
113.80.0.0
121.13.0.0
113.77.0.0
14.156.0.0
14.220.0.0
183.22.0.0
113.102.0.0
14.219.0.0
14.222.0.0
14.221.0.0
223.74.0.0
124.194.0.0
14.217.0.0


192.168.2.2
05/02/17
12:00 AM CST
24 Hour(s)
05/03/17
12:00 AM CST
192.168.2.2
192.168.2.2 as Server
接口和应用排名基于 ServerOctets
Filters ⇒ None
Search Result
Activity Map
Interfaces (2)
Applications (4)
Client / Client Communities (596)
VLANs (5)
VLANs...
VLAN 102
VLAN 105
VLAN 103
VLAN 104
VLAN Unknown

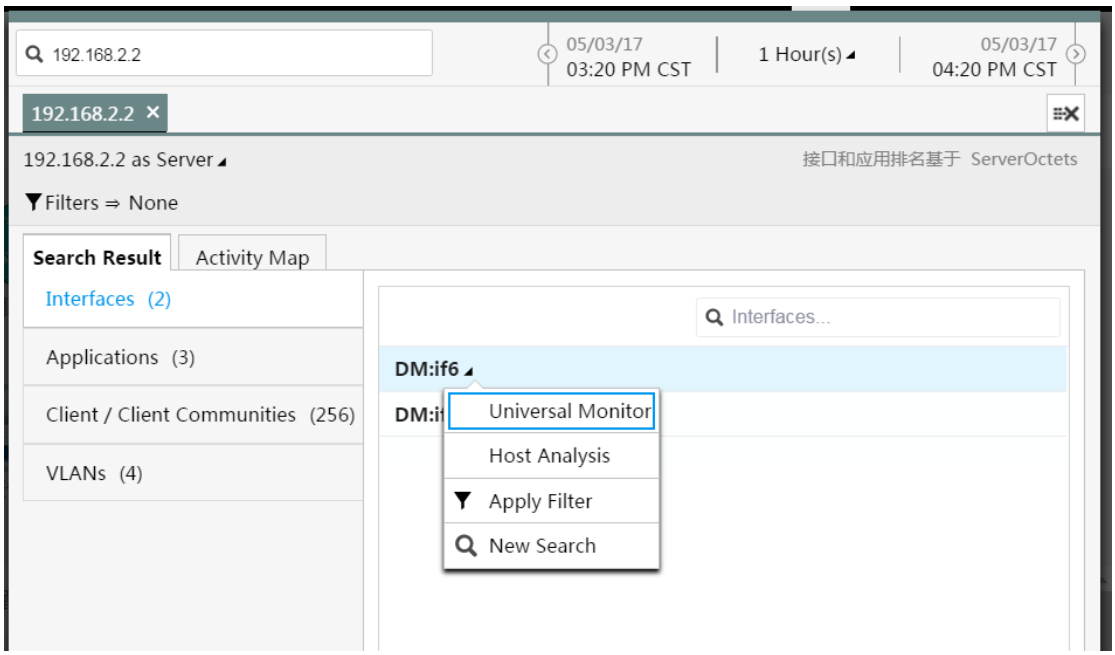
可更改搜索时间段

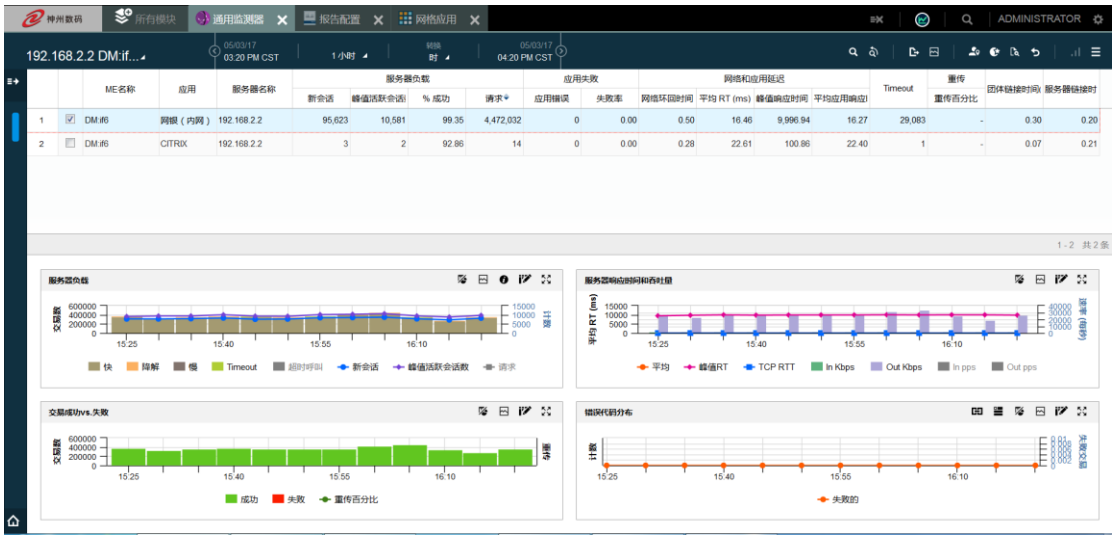


点击“Activity Map”可直接查看该主机在接口下的活跃时间，绿色方块代表该一小时里该主机有通信，灰色则无；



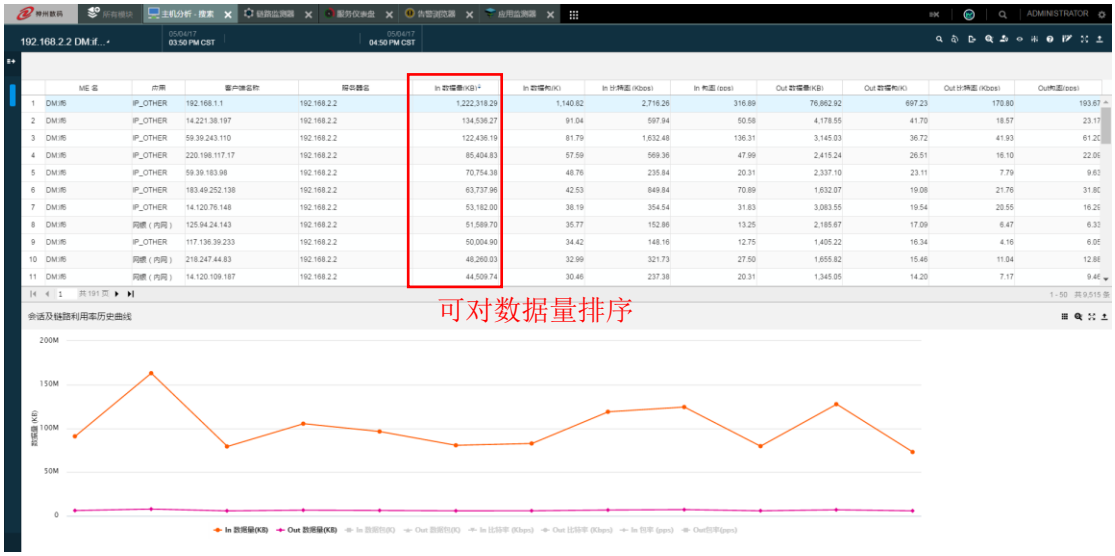
在“全局搜索”中可使用“Universal Monitor”去监测主机，如图：





还可以用“Host Analysis”去对主机进行分析，如图：

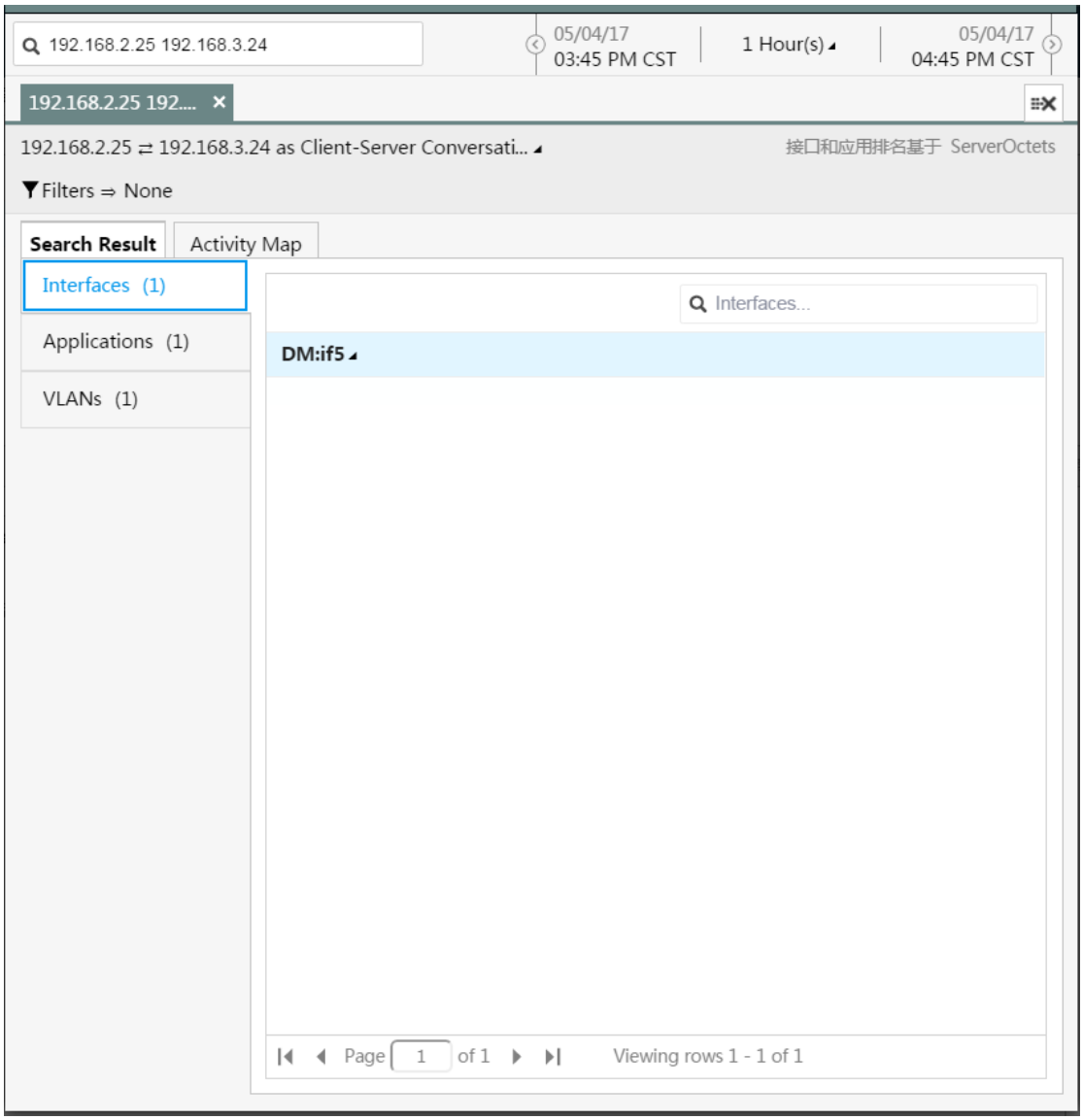
在 Host Analysis 界面有主机相关应用层通信对的进出流量信息，对其进行排序后便能得出流量排行 TOP N 的应用层通信对



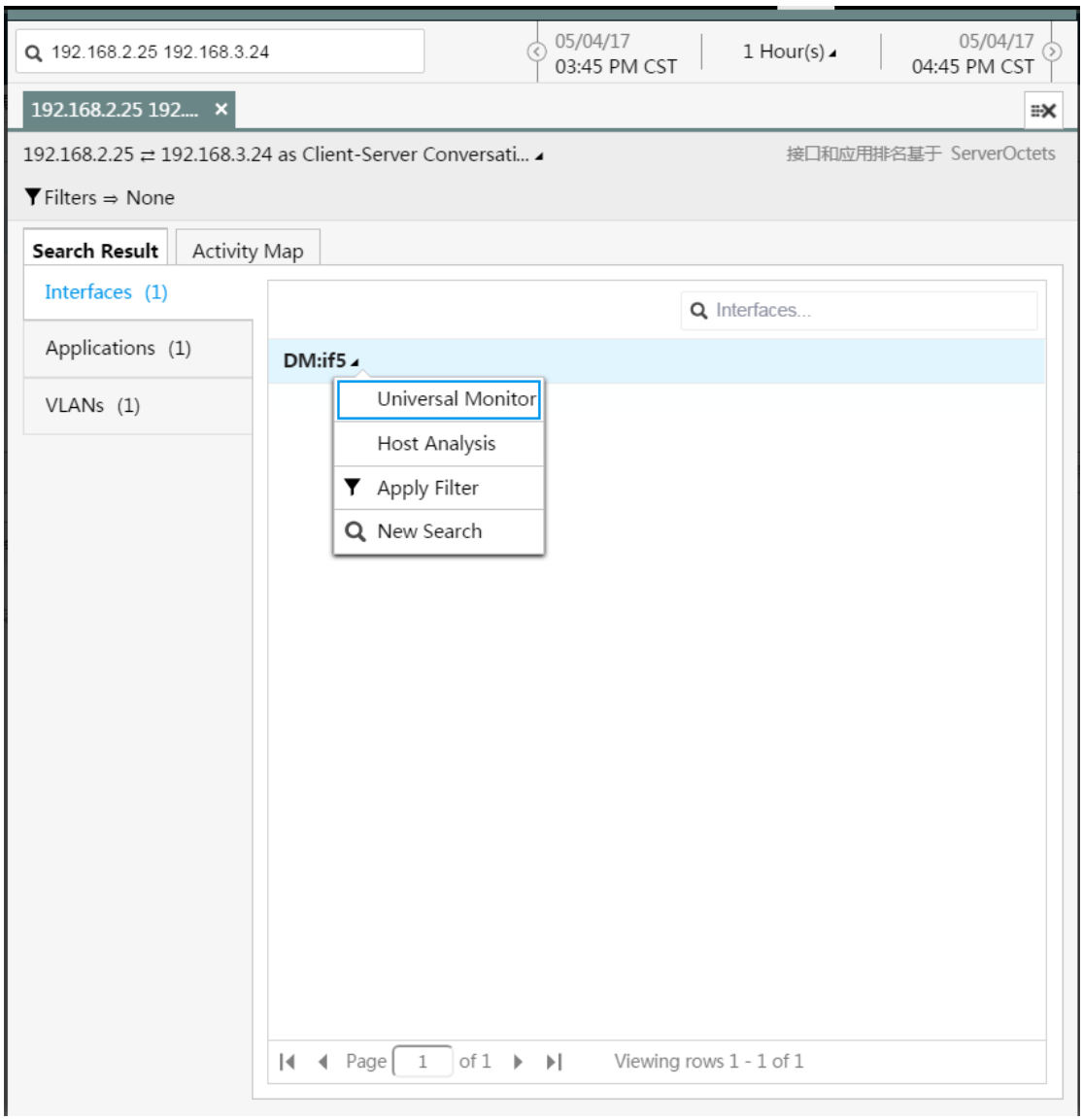
上述两种监测方式均可以点击图表中的图标 来进入数据包解码界面。

3.4.2 通讯对搜索

在搜索框中输入通信对（两个 IP 地址间以空格分隔）进行搜索，与主机搜索类似，能查看通信对所在接口、应用信息、Activity Map 等信息；

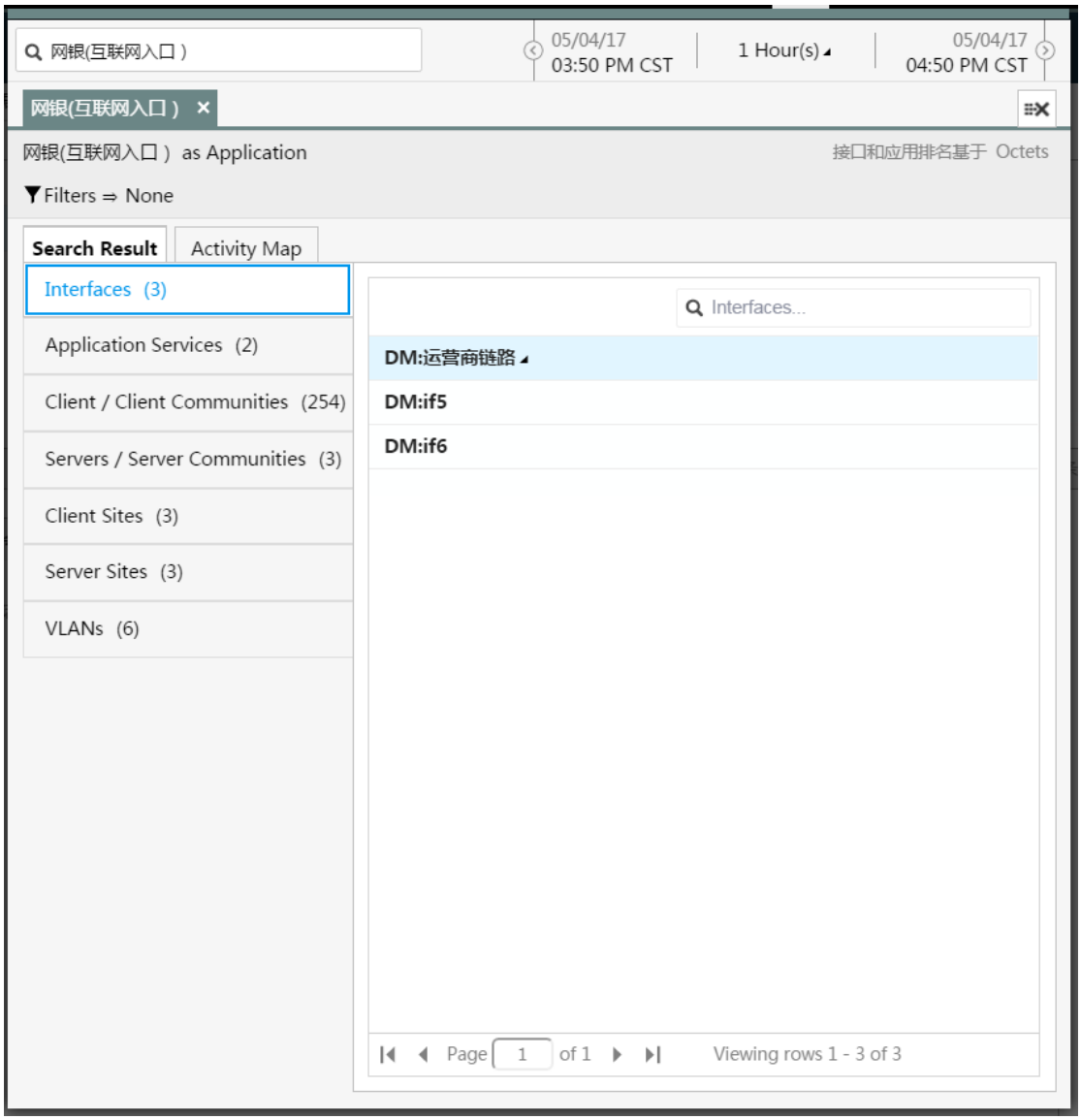


同样地，可使用通用监测器以及主机分析两种方式来查看该通讯对

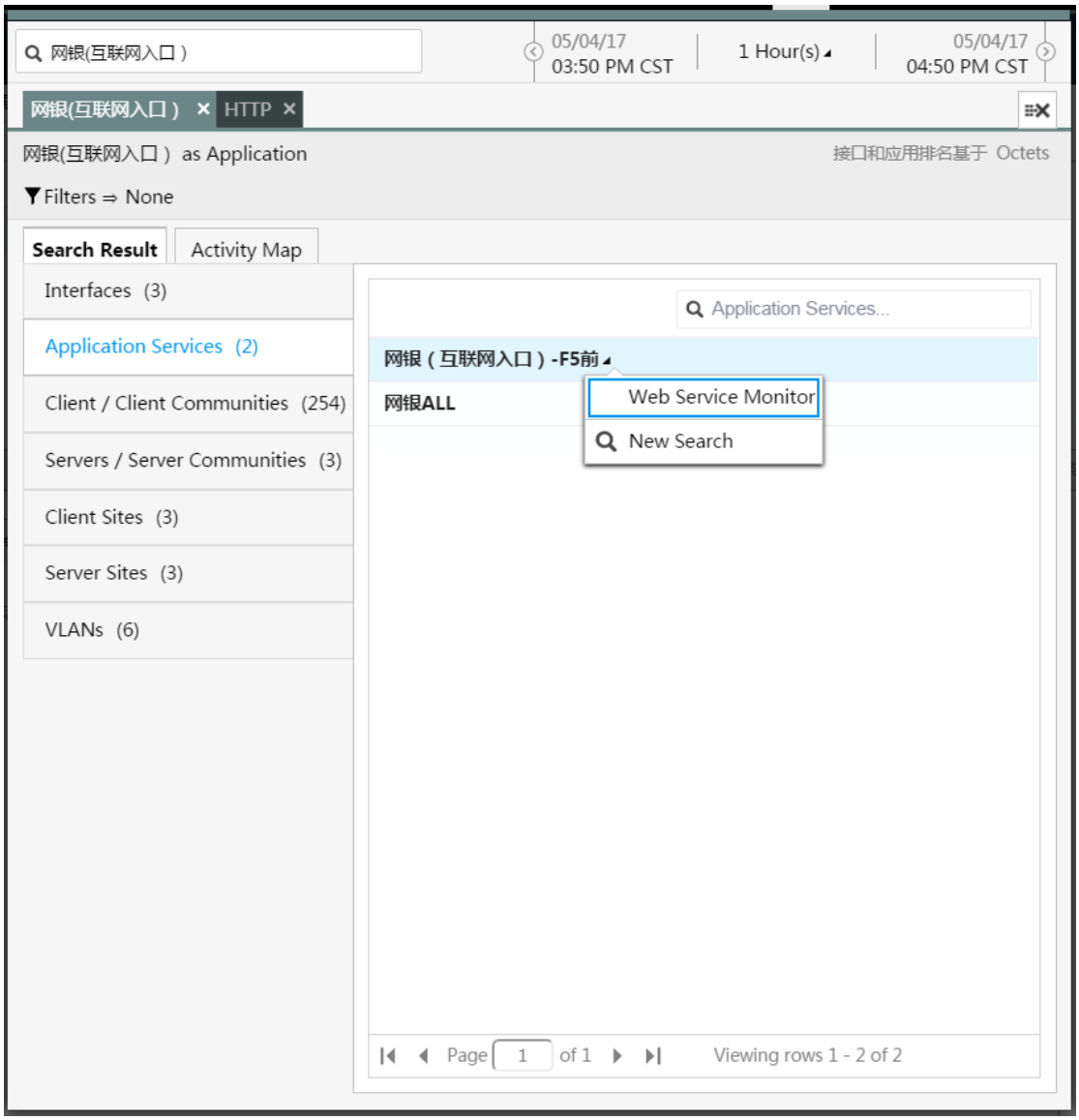


3.4.3 应用搜索

在搜索框中输入应用名称进行搜索,以应用网银(互联网入口)为例,会展示与“主机搜索”、“通讯对搜索”类似的信息，如所在接口、VLAN、应用信息、Activity Map 等信息

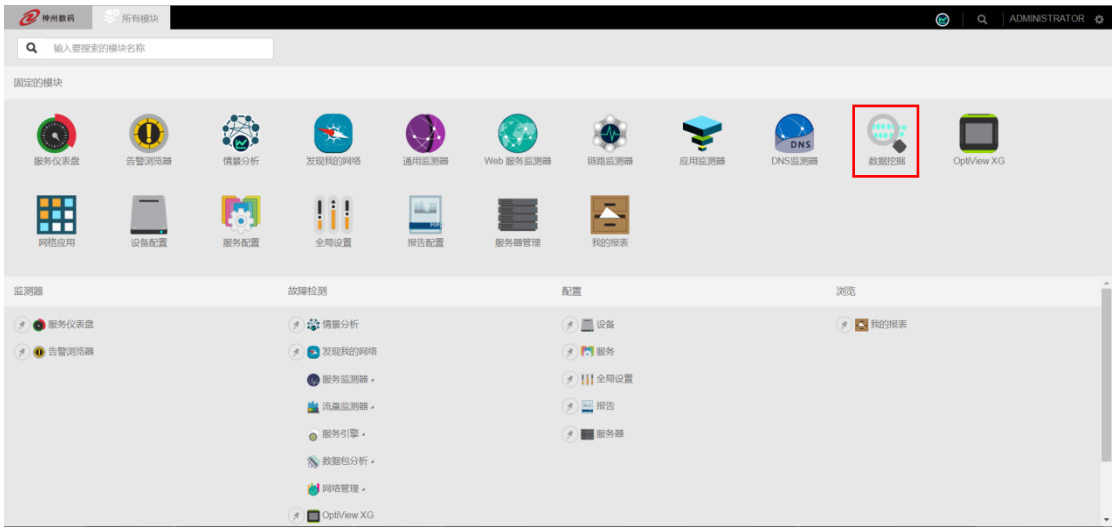


对于特定应用，可用应用相关的监测器去查看，如应用网银（互联网入口）为 web 应用，可用 web 服务监测器去查看。



3.5 数据包挖掘

在“所有模块”上选择“数据挖掘”，进入数据包捕获模块，对网络中的数据包进行抓取；

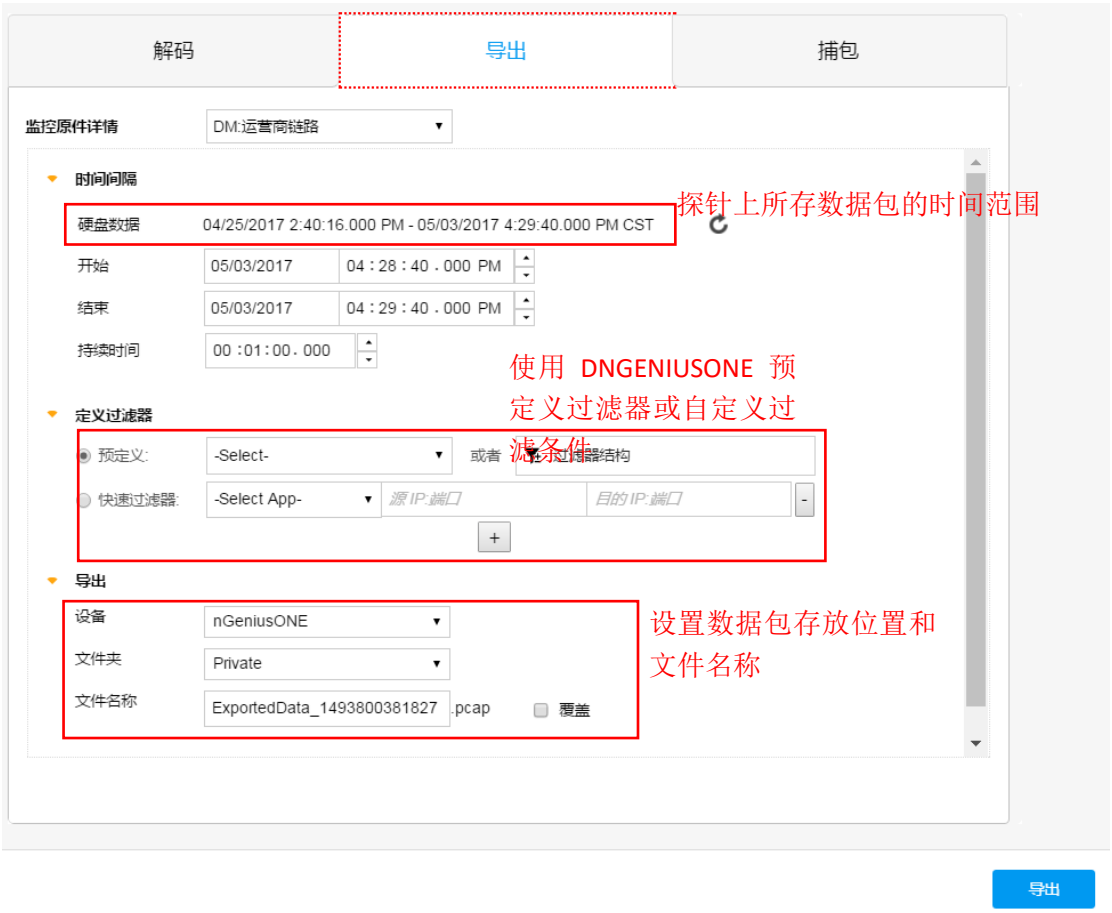


选取对象（待抓取数据包的接口，如运营商链路；或网络服务，如电信 1、联通 1 等），选择并选择对应的动作（解码、导出、捕包三种）

3.5.1 历史数据包输出

选取对象，选择“导出”，对已经储存在探针当中的数据包进行输出；

在此页面中，可以设定所输出数据包的名称、保存目录、格式以及时间段（该时间段不可超出探针上所存数据包的时间范围）；



除了使用 nGeniusONE 预定义的过滤器外，用户还可以自定义过滤条件。可在“快速过滤器”中对已经定义过的应用或者源目 IP 地址+端口进行过滤；也可以点击“过滤器结构”来自己编写过滤条件，如下图：

Pattern[74-77]==55534552→指定 pattern 55534552

802.1q.vlan_id==12→指定 vlan 12

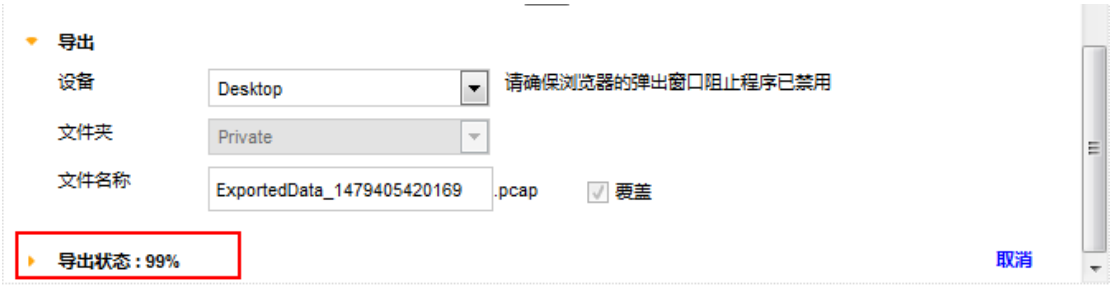
Ip.addr==10.2.105.109→指定主机 10.2.105.109

Tcp.port==80→指定 TCP 80 端口

数据包有三种保存位置，nGeniusONE 服务器（private、share 两个目录）、Infinistream 探针（private、share 两个目录）和用户设备本地，当设定好具体输出的目标位置后，点击“开始”即可将 Trace 文件输出到需要查看的客户端指定目录。

（注意在将数据包下载到本地的时候浏览器会弹框提示设置数据包存放位置，请确保浏览器弹窗功能已启用）

在导出的过程中会显示目前的导出状态

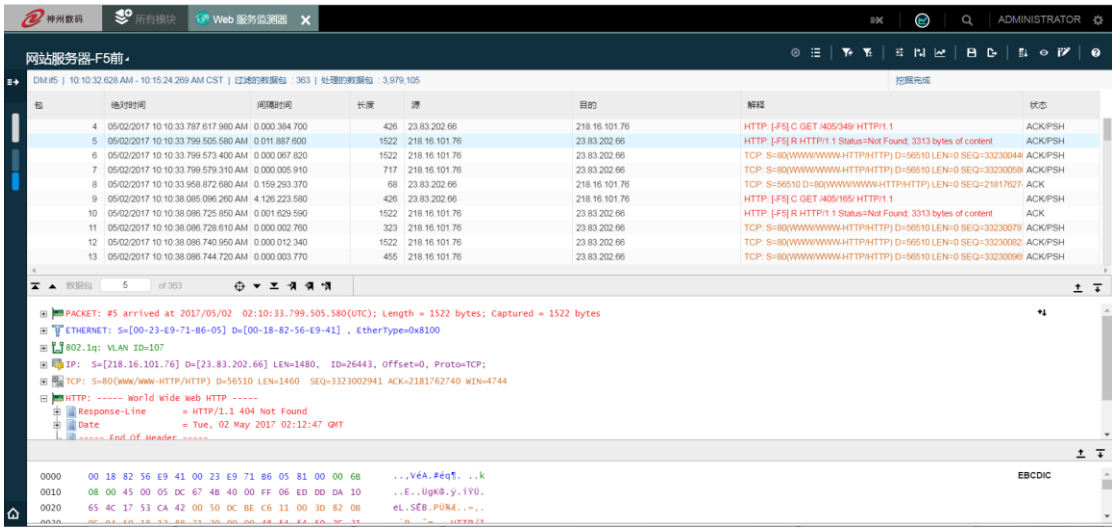


缺省保存的文件格式为.cap，可以用解码软件进行分析。

3.5.2 历史数据包在线解码

在解码界面中，可以对探针上存储的历史数据包进行查看分析；

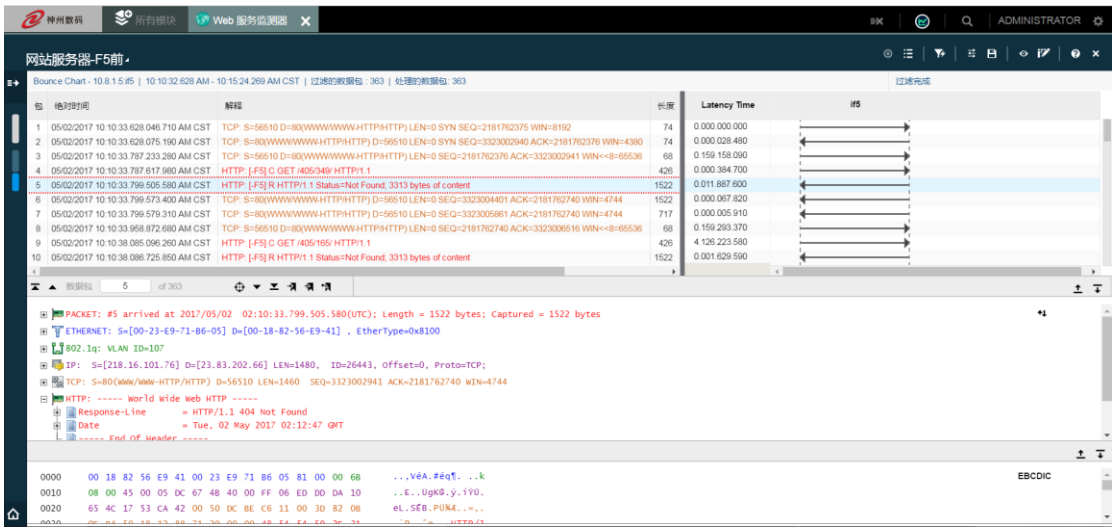
设置好时间和过滤条件和点击“解码”进入数据包解码界面，如图：



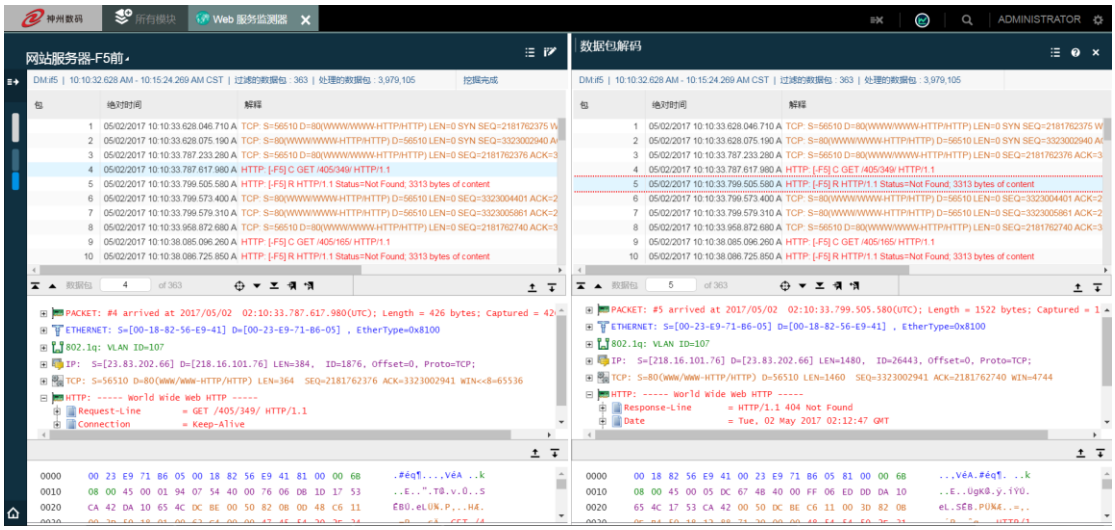
在解码界面支持多样功能，如：

过滤器（工具栏中的  ），支持使用语法手动编写过滤器，如下图中过滤出 192.168.1.93-218.94.124.41 的端口 8765 以及端口 23557 的数据包。

跳动图表（工具栏中的  ），显示数据包传输的延时信息以及传输方向。

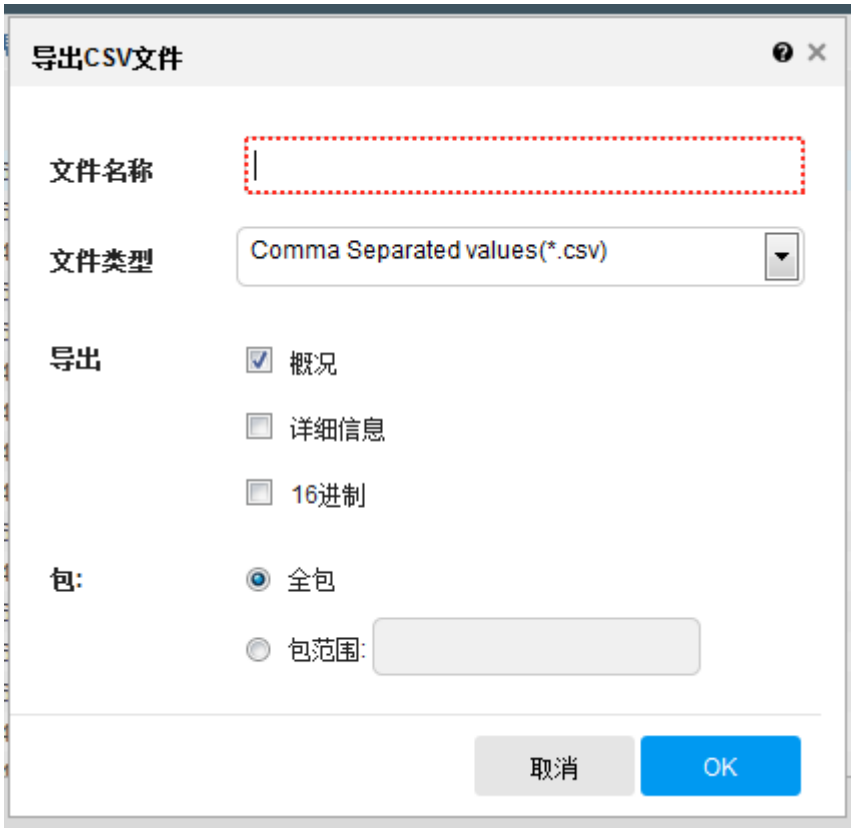


分屏查看数据包（工具栏中的  ），可用于对比两个关联的数据包，如请求包和对应的响应包。

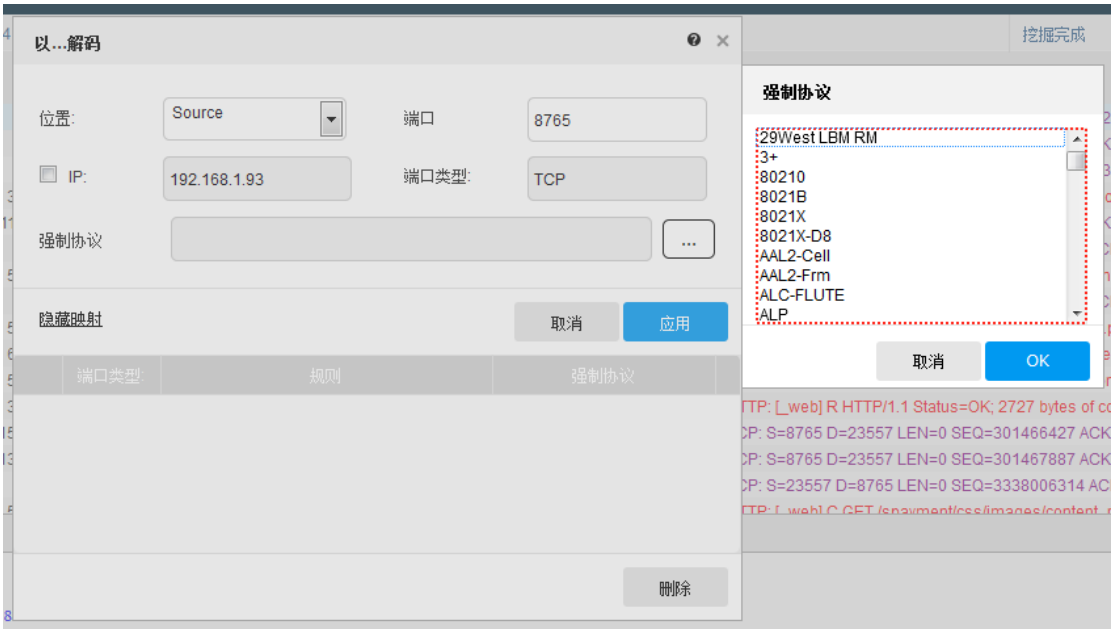


保存数据包  ，将抓取出来的数据包保存到指定位置；

导出成 CSV 文件  ，导出后以.csv 文件格式查看

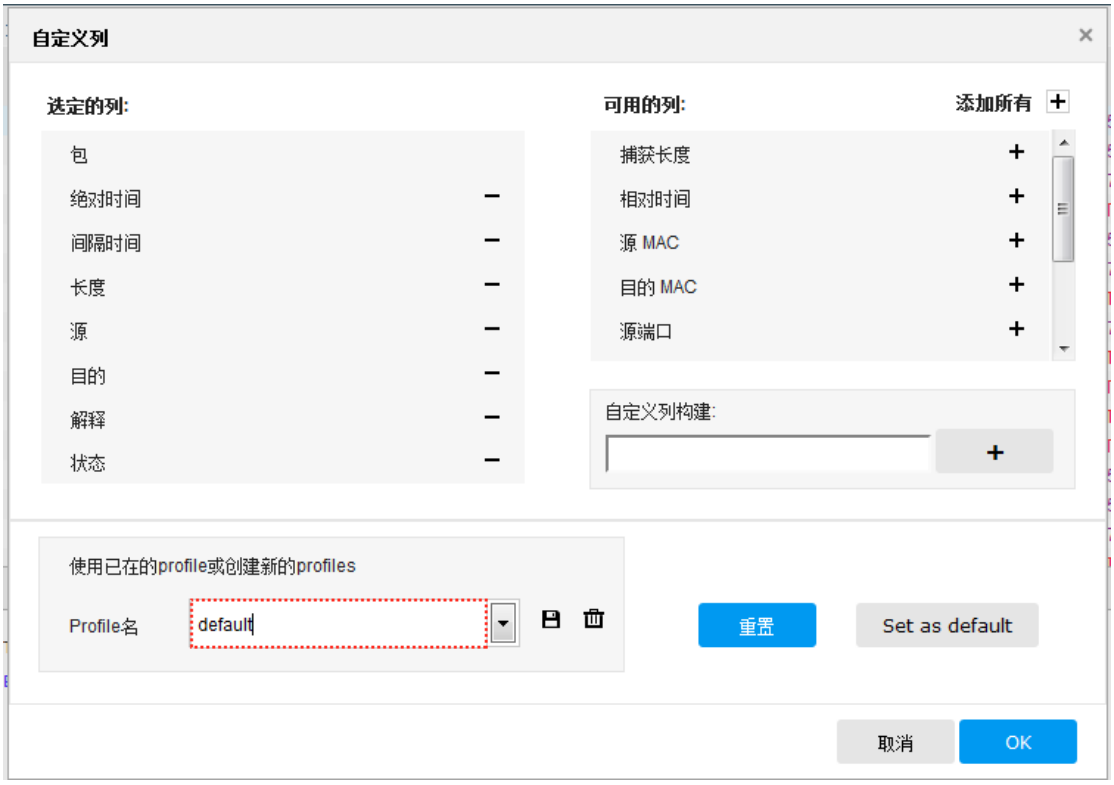


以...启动解码  ，针对协议来过滤数据包；

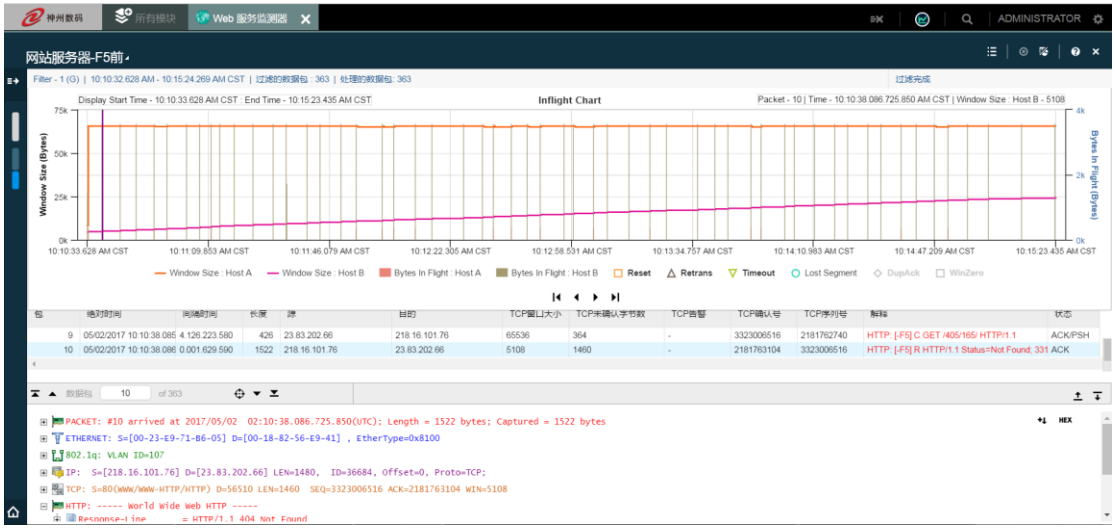


查看选项  ，更改数据包解码界面的查看方式；

Measure，添加或删减数据包解码界面查看项；



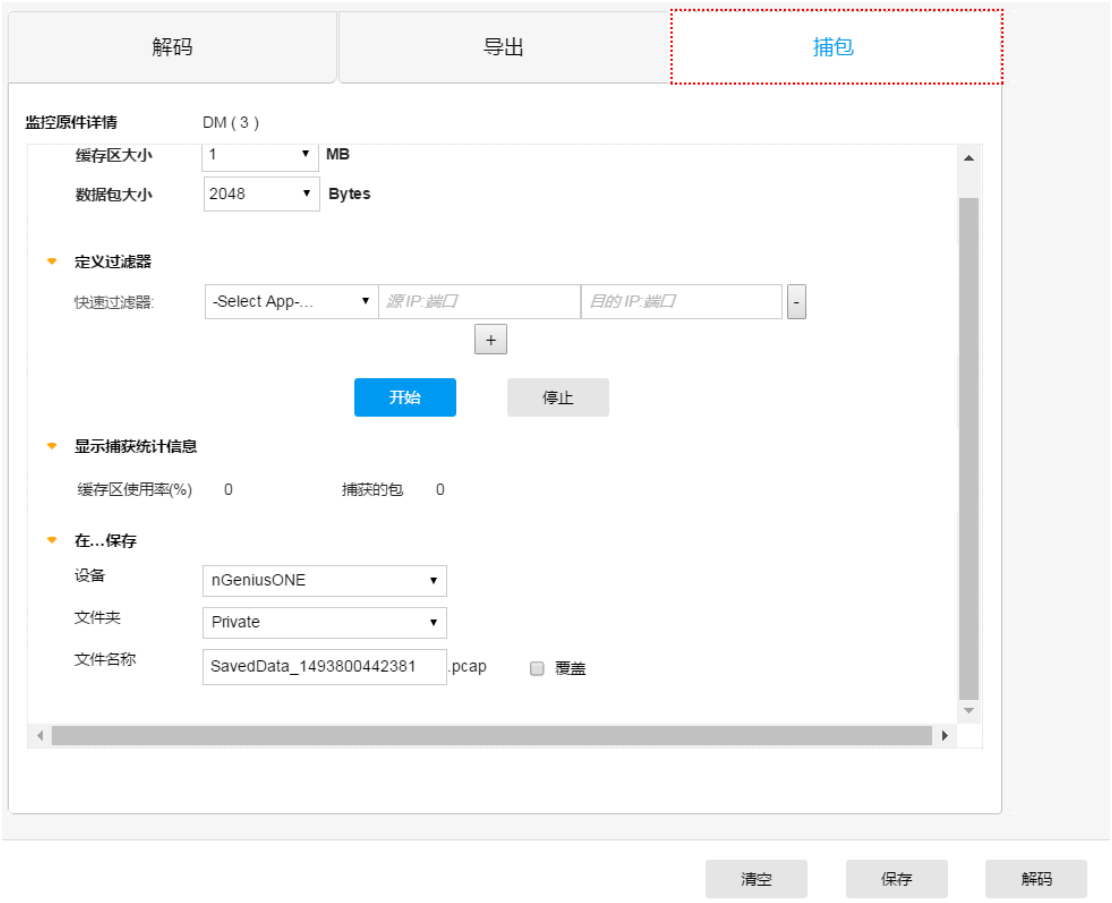
增强解码功能（工具栏中的  ），将 TCP 分析的部分参数（如 TCP 窗口大小、重传数等）与数据包解码界面以图表形式联合展示。



3.5.3 实时数据包获取

在捕获页面中，可以设定数据包的过滤条件，即按照 IP 或者所定义的应用来进行数据包的

捕获；还可以选择解码文件的名称、保存位置以及所要捕获的数据大小等（切片大小改为“0”表示抓全包）；



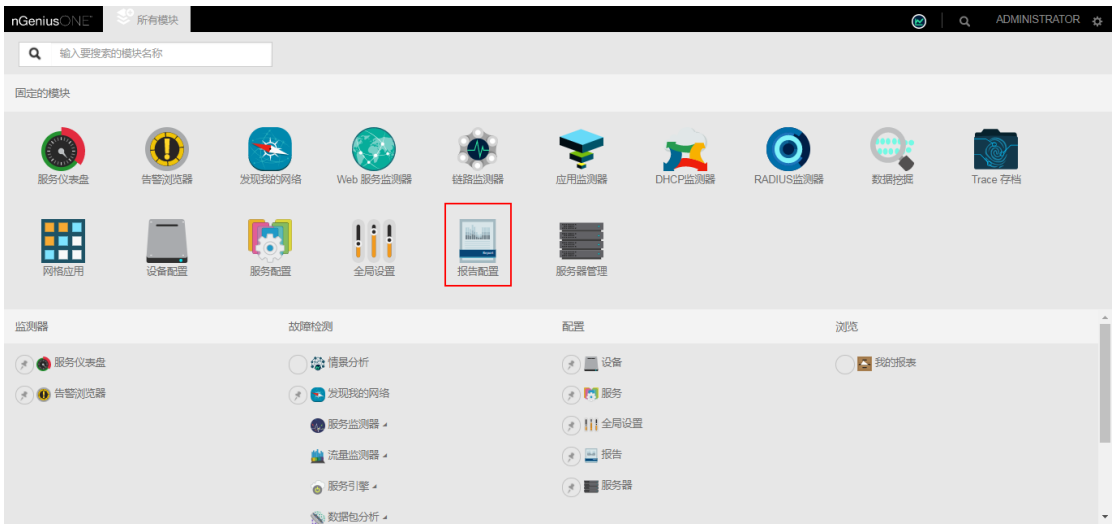
点击“开始”按钮即可启动数据包捕获，可以通过下方的状态信息获知已捕获包的数量和可用缓冲区等信息。当已捕获足够的数据包，点击“停止”按钮停止捕获。当停止捕获数据包后，可以选择“保存”保存 Trace 文件到 nGeniusONE 服务器指定的目录，也可以选择“解码”查看数据包内容，最后完成数据包分析后点击“清空”来释放用于捕包的缓存空间。

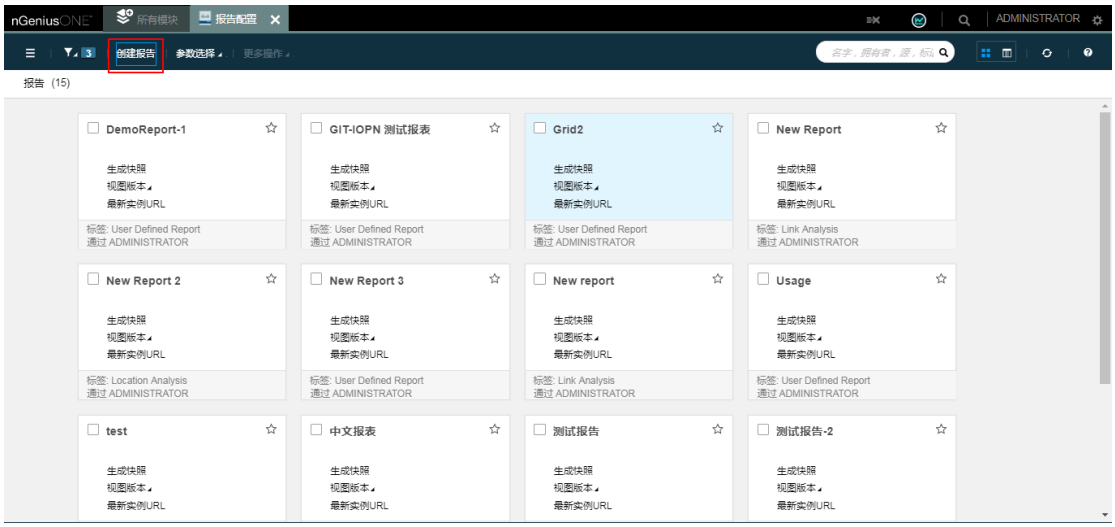
3.6 报表

nGeniusONE 系统支持定制监控内容相关报表，并通过邮件发送，方便运维人员定期了解网路状态。

3.6.1 定制报表

在“所有模块”下进入“报告配置”，然后在配置界面点击“创建报告”来新建报表



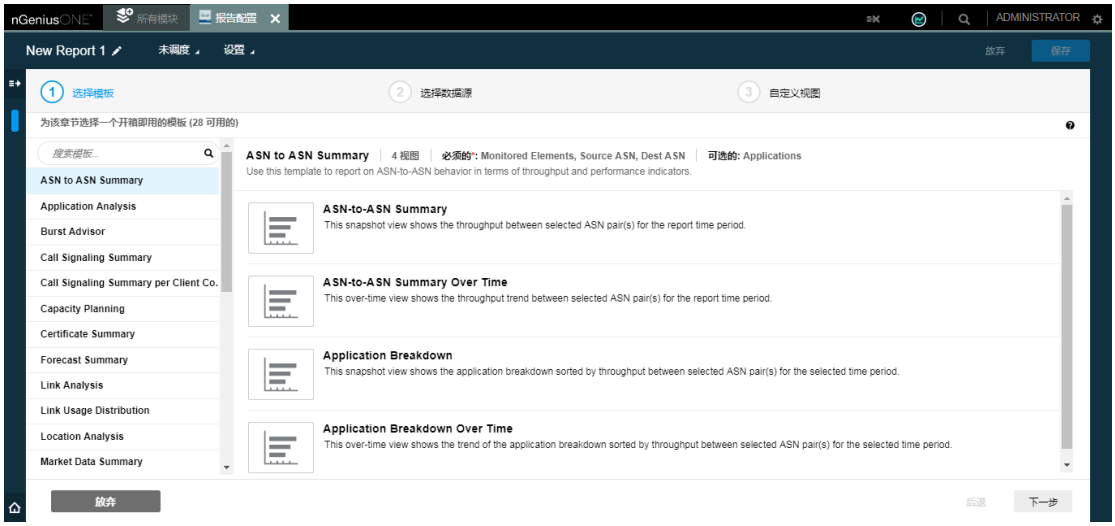


新建报表有三个步骤：

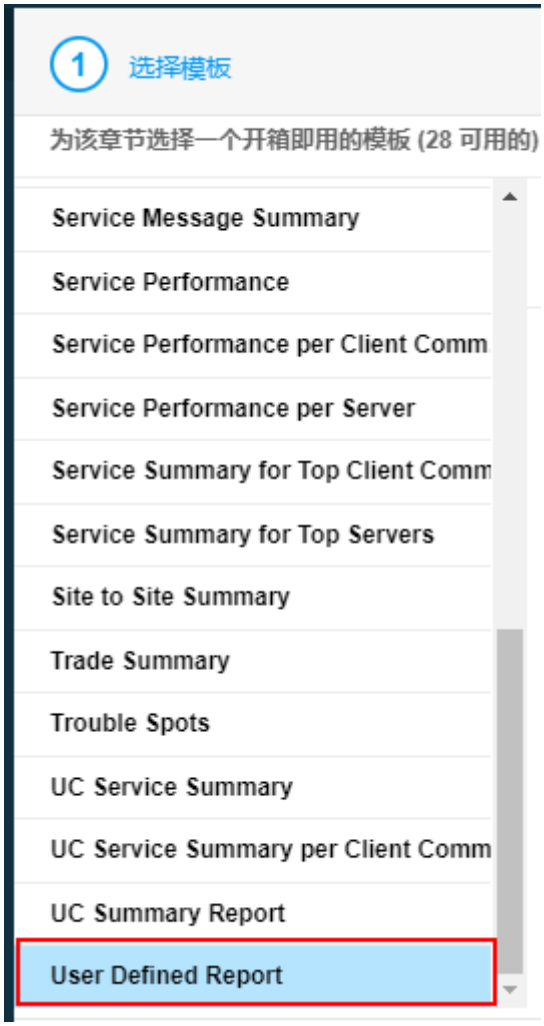
① 选择模板

nGeniusONE 中有大量模板可供用户选择，用户选择模板之后右方界面有该模板对应的视

图及解释



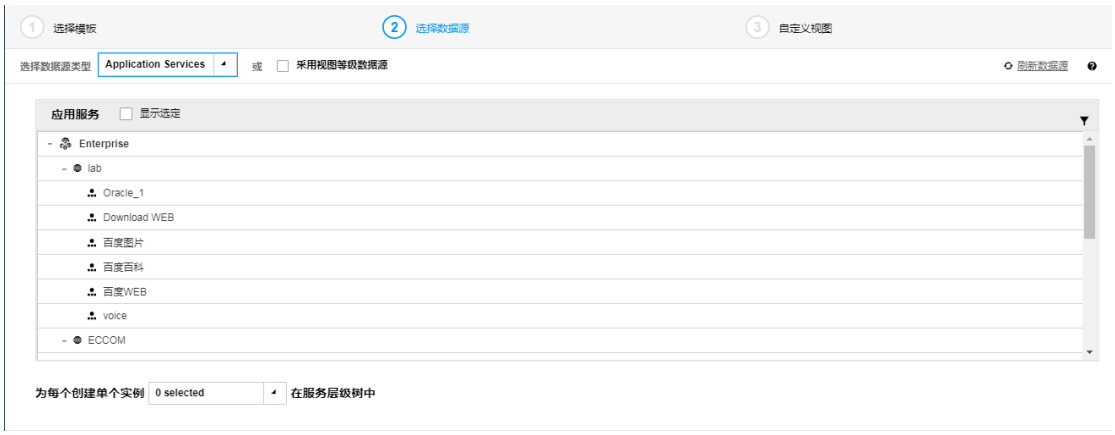
如果已有的模板不能满足用户需求，也可以选择自己定义报表视图



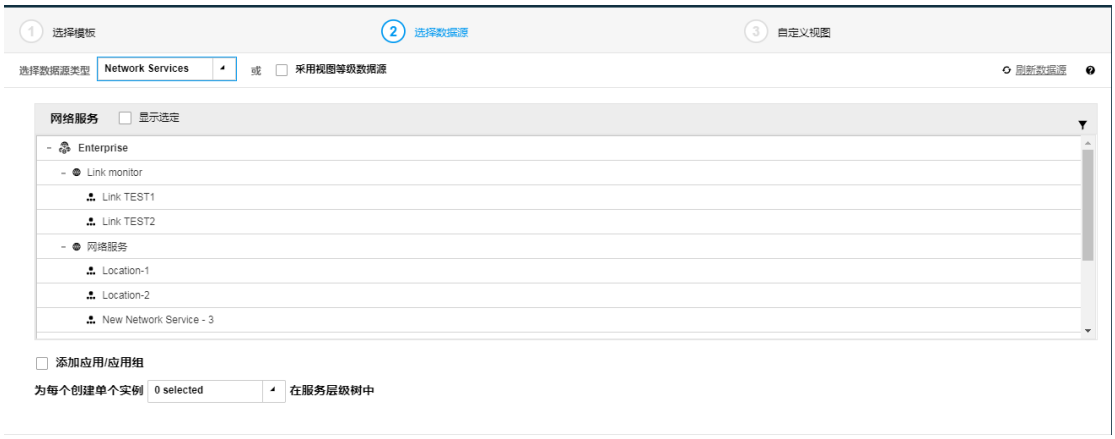
② 选择数据源

为报表选择一个数据源，选择对象可以是“应用服务”、“网路服务”和具体探针接口

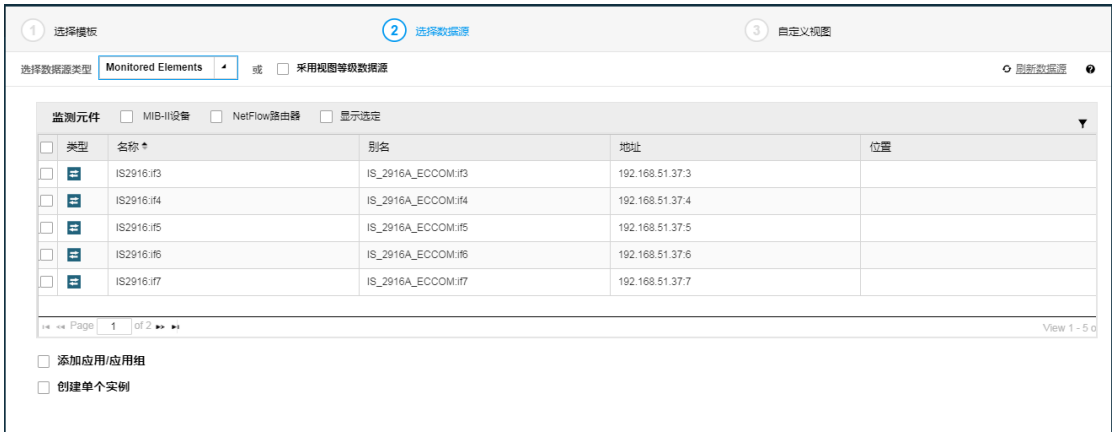
应用服务：



网络服务

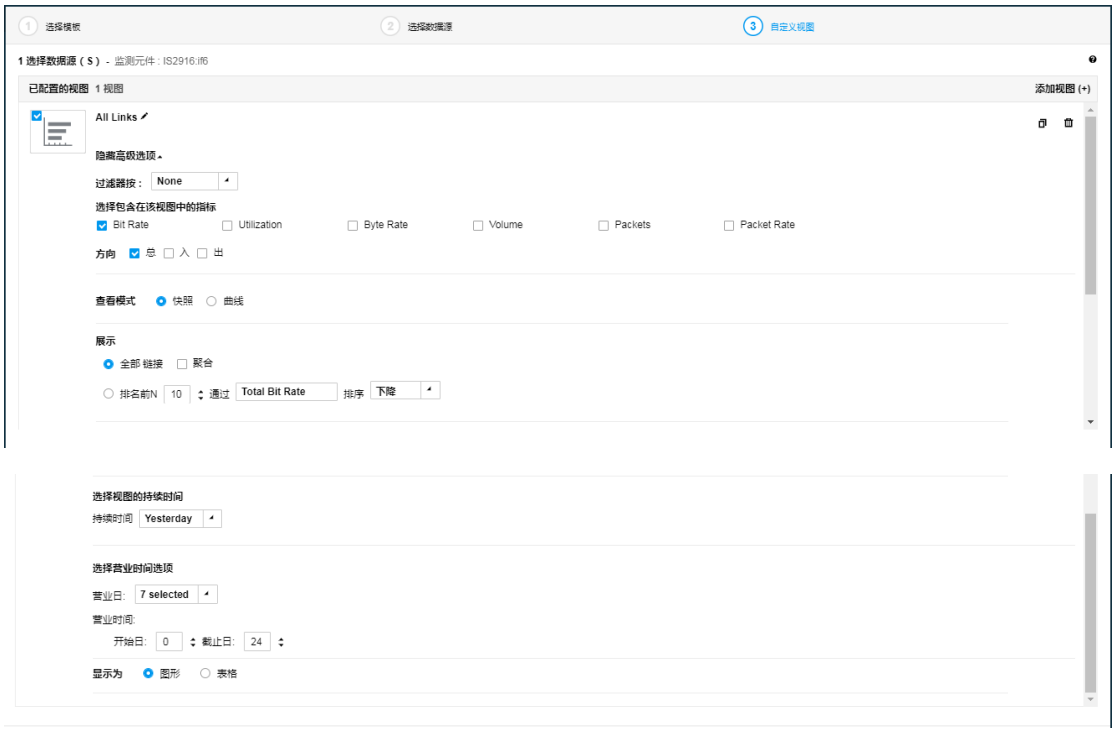


探针接口



③ 自定义视图

最后对报表的每个视图进行调整，选择报表需要展示的数据、展示模式以及时间跨度

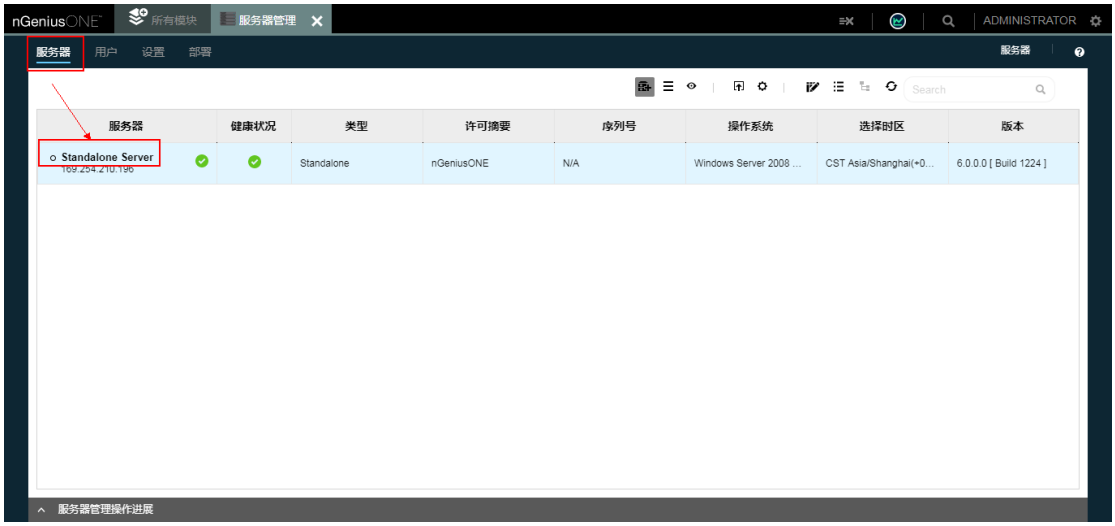


定制完成后点击“结束”→“保存”，完成报表定制

3.6.2 定期发送报表

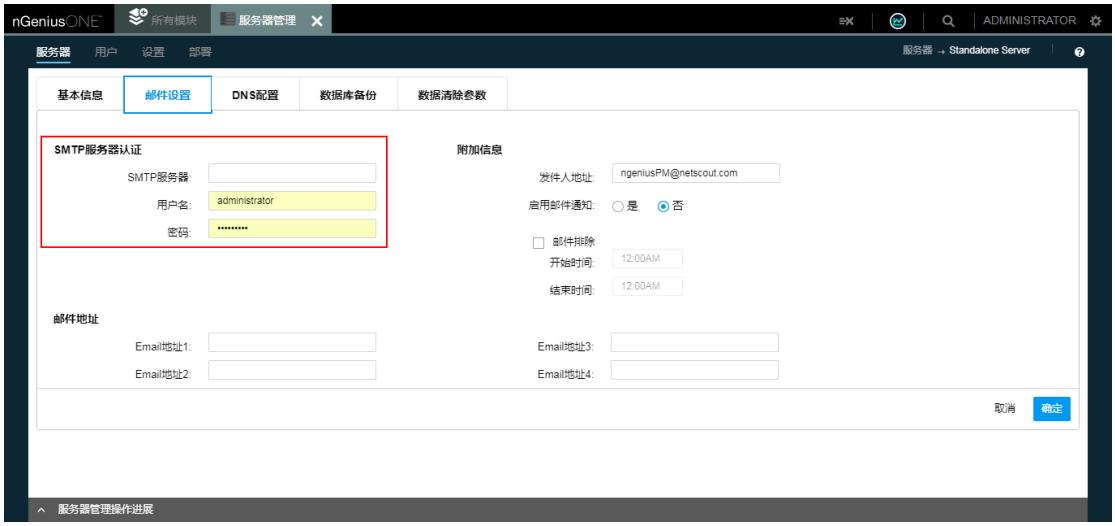
报表可以设置定期通过邮件向外发送，在“所有模块”下进入“服务器配置”

依次点击“服务器”→“Standalone Server”→“邮件设置”

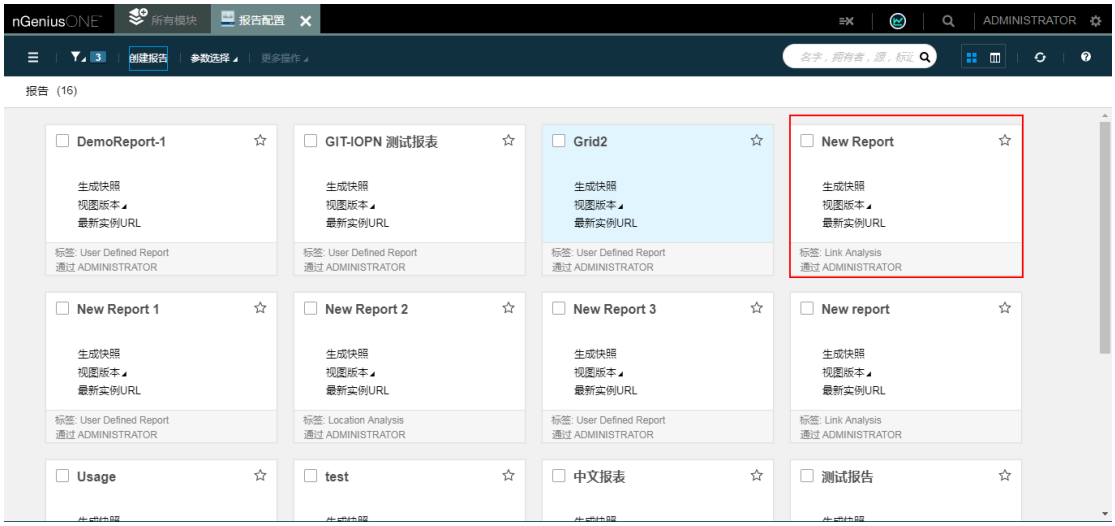


在“SMTP 服务器认证”部分，填入网络中的 SMTP 服务器地址。若 SMTP 需要进行认证，还需填入认证用户的用户名/密码，让 nG1 系统通过服务器认证。

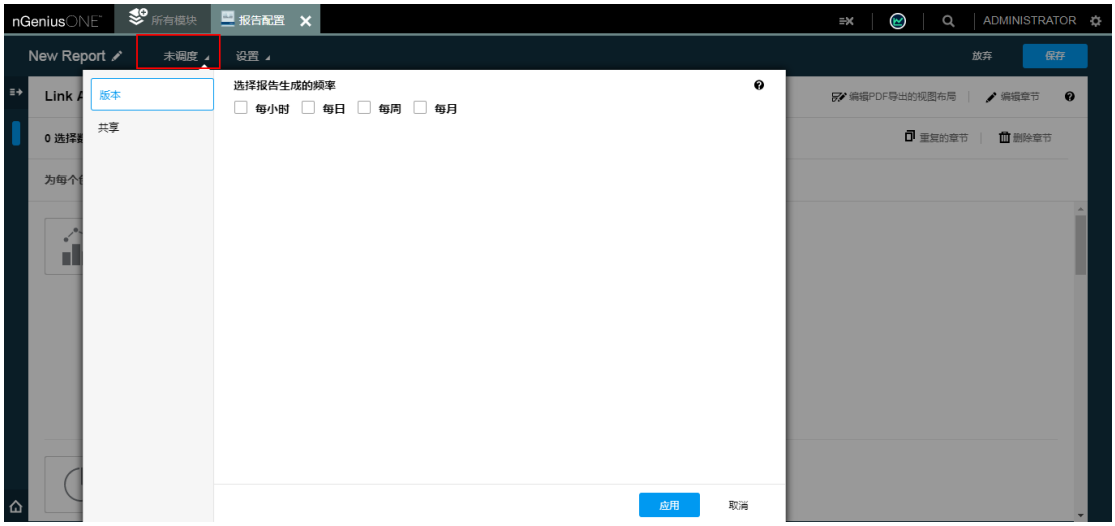
（注：需要进行认证的情况下，需要在 nG1 服务器后台的配置文件“serverprivate.properties”中添加以下语句：mail.smtp.auth=true）



完成 SMTP 设置后，再跳转至“报告配置”界面，点击要定期发送的报表，对报表配置进行修改



点击左上方的“未调度“字样，打开下拉菜单，在菜单中选择报表生成周期



再到“共享”菜单中设置发送地址以及内容：

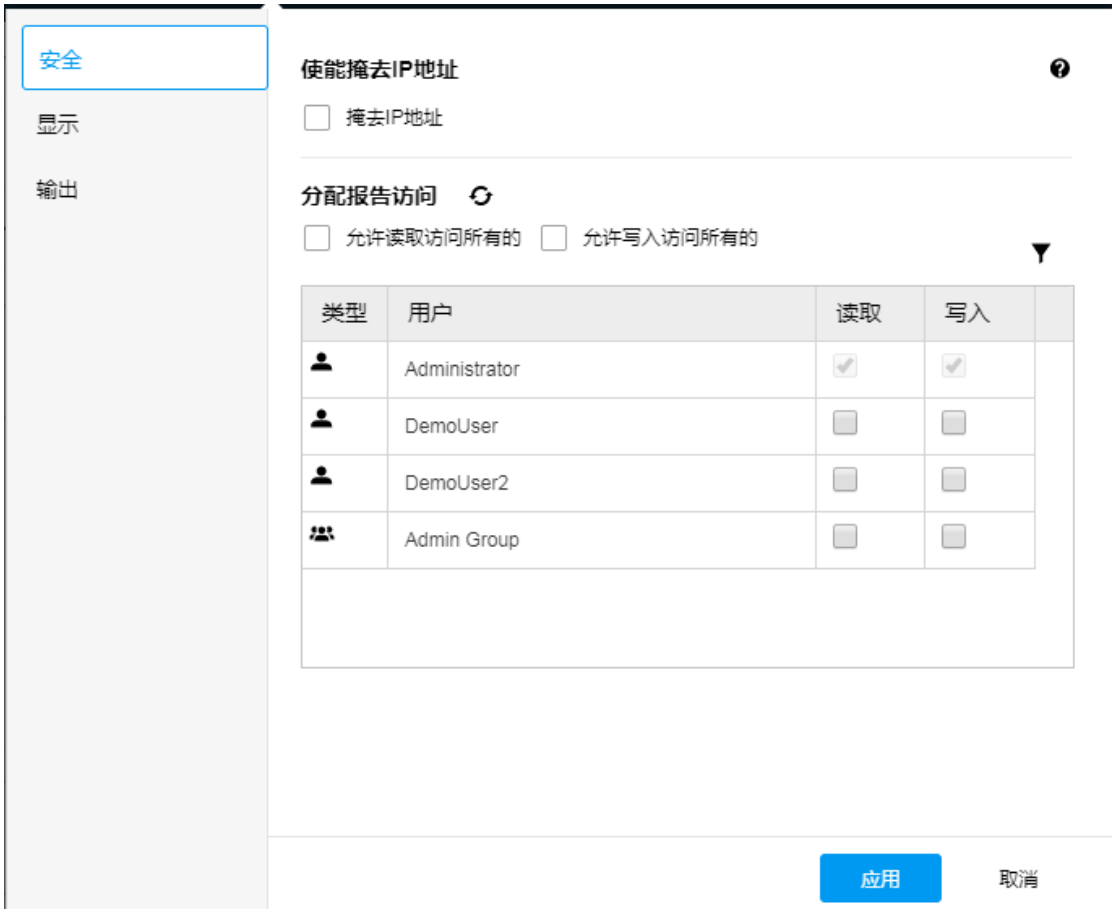
① 勾选“启用电子邮件传送”

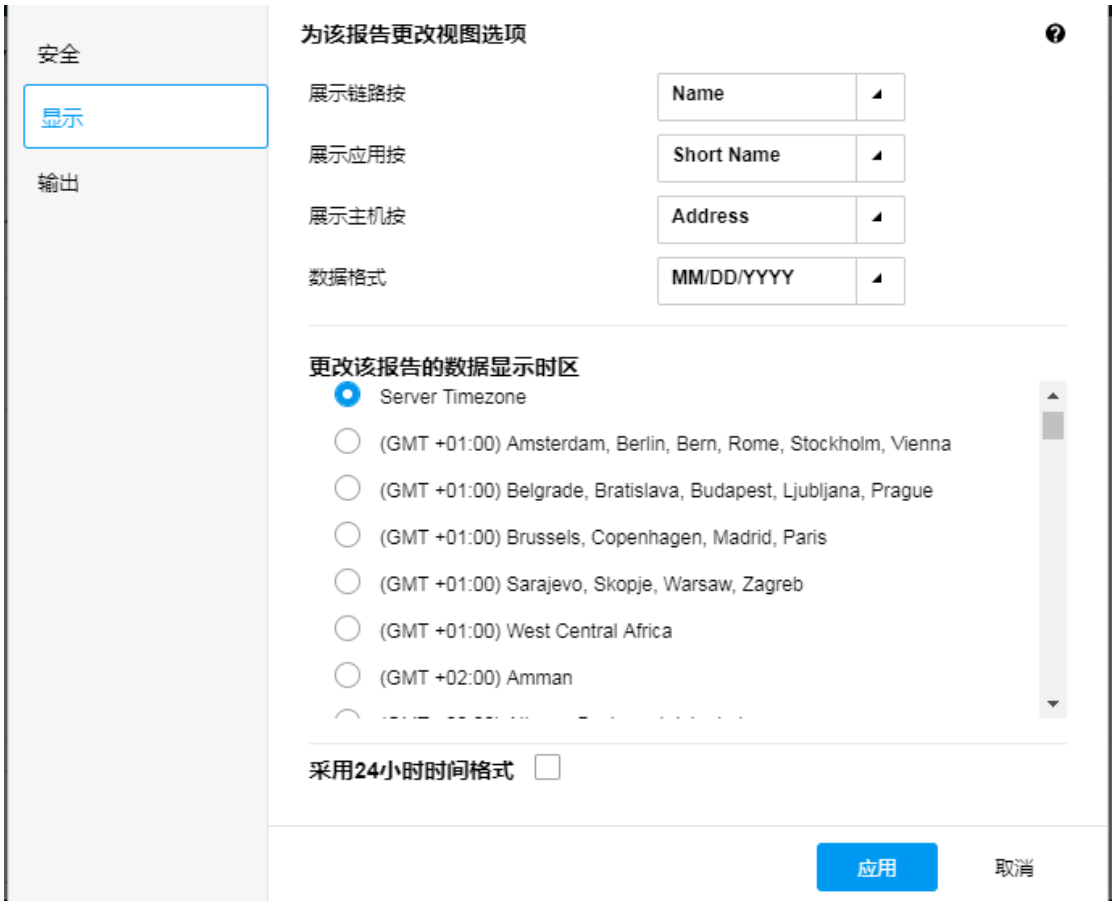
② 设置发送地址和接收地址

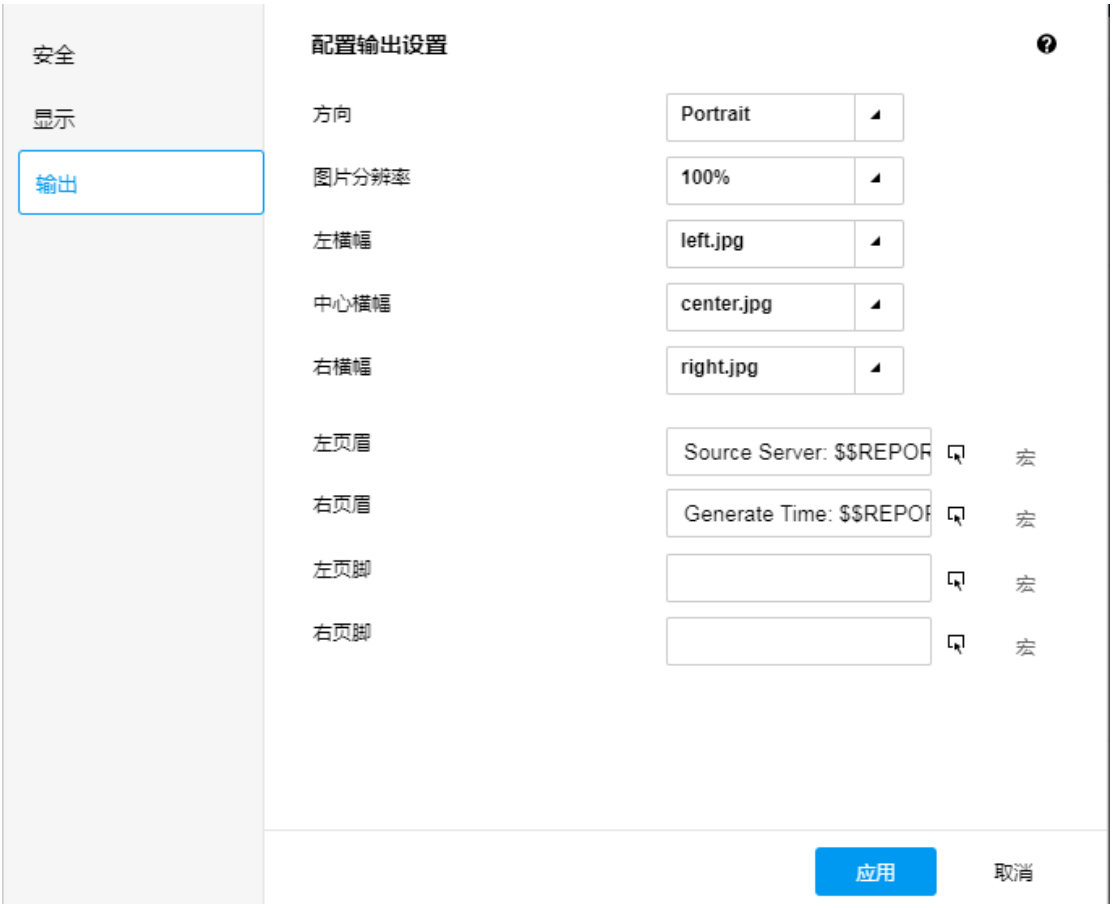
③ 编辑邮件主题和邮件内容

④ 选择发送格式

最后在“设置”菜单中对附件内容进行调整


安全
显示
输出
使能掩去IP地址
掩去IP地址
分配报告访问
允许读取访问所有的
允许写入访问所有的
类型
用户
读取
写入
Administrator
DemoUser
DemoUser2
Admin Group
应用
取消


安全
显示
输出
为该报告更改视图选项
展示链路按
Name
展示应用按
Short Name
展示主机按
Address
数据格式
MM/DD/YYYY
更改该报告的数据显示时区
Server Timezone
(GMT +01:00) Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna
(GMT +01:00) Belgrade, Bratislava, Budapest, Ljubljana, Prague
(GMT +01:00) Brussels, Copenhagen, Madrid, Paris
(GMT +01:00) Sarajevo, Skopje, Warsaw, Zagreb
(GMT +01:00) West Central Africa
(GMT +02:00) Amman
采用24小时时间格式
应用
取消


安全
显示
输出
配置输出设置
方向
Portrait
图片分辨率
100%
左横幅
left.jpg
中心横幅
center.jpg
右横幅
right.jpg
左页眉
Source Server: $$REPOR
宏
右页眉
Generate Time: $$REPOR
宏
左页脚
宏
右页脚
宏
应用
取消

4. nGeniusONE 应用性能分析配置

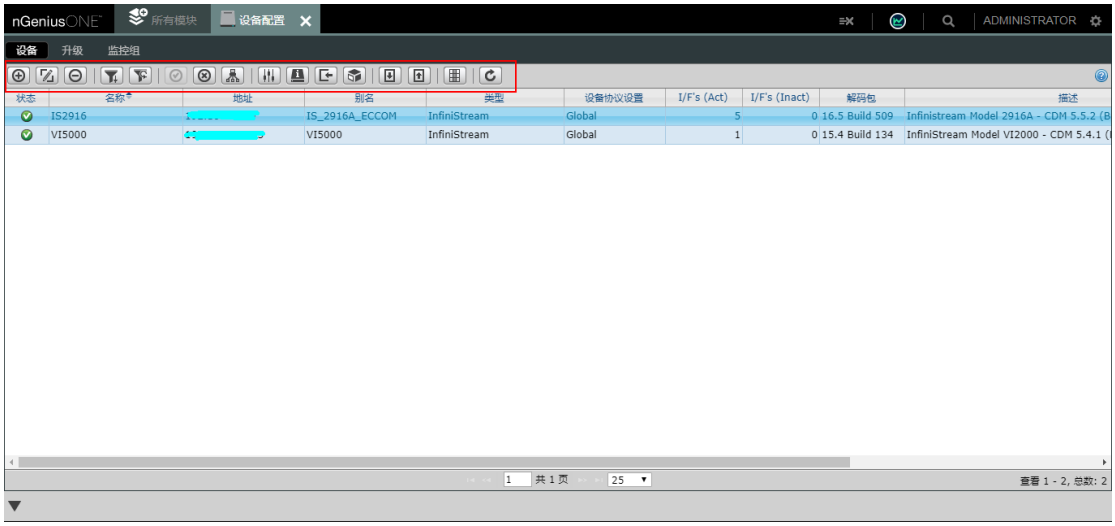
一般情况下，使用 nGeniusONE 需要配置以下内容：

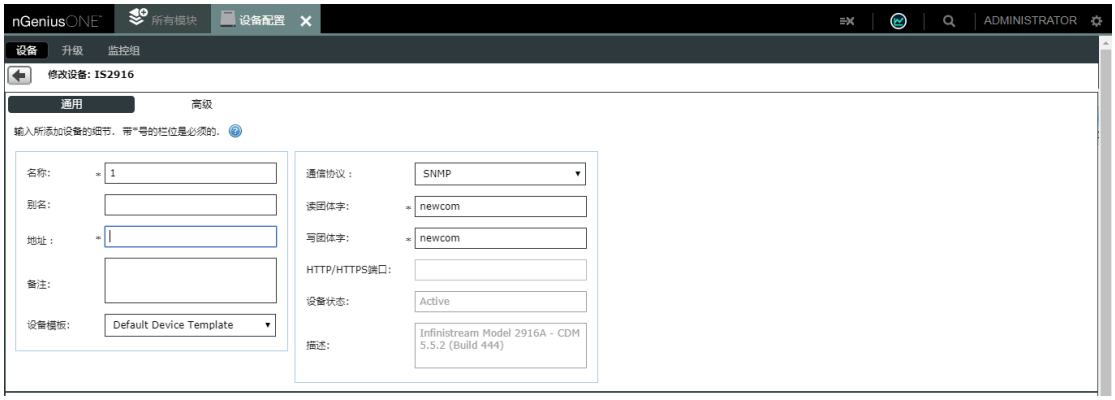
①添加探针→②配置应用→③配置全局设置→④配置服务域和服务→⑤配置服务告警

4.1 添加探针

在“所有模块汇”中选择“设备配置”模块，该模块可用于接管网络中的探针设备，对其名称、接口、关联 site 等信息进行配置

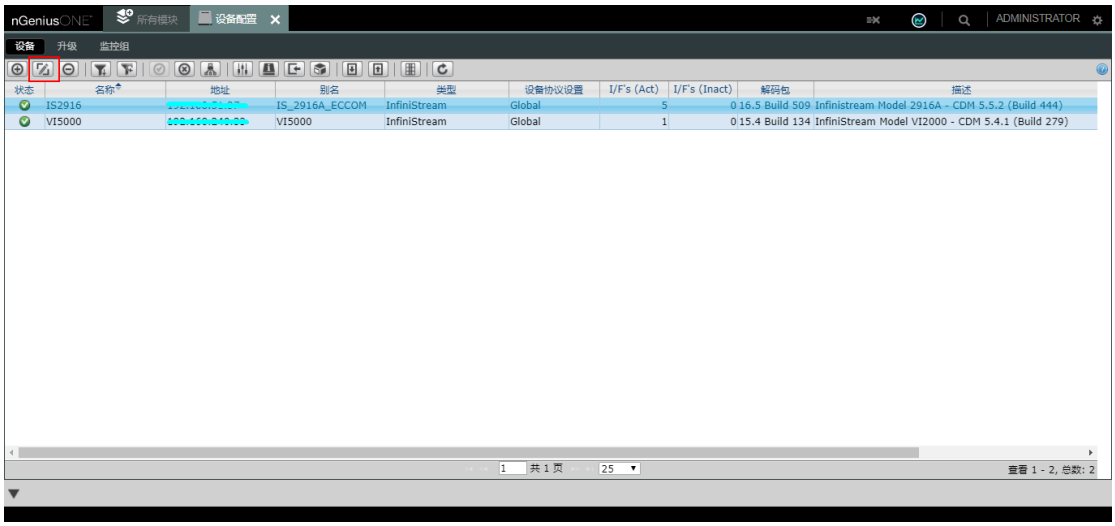
在“设备配置”界面里单击，输入所要添加的设备名称、别名、IP 地址、读写团体字等，然后点击确认，就完成了对新设备的添加；

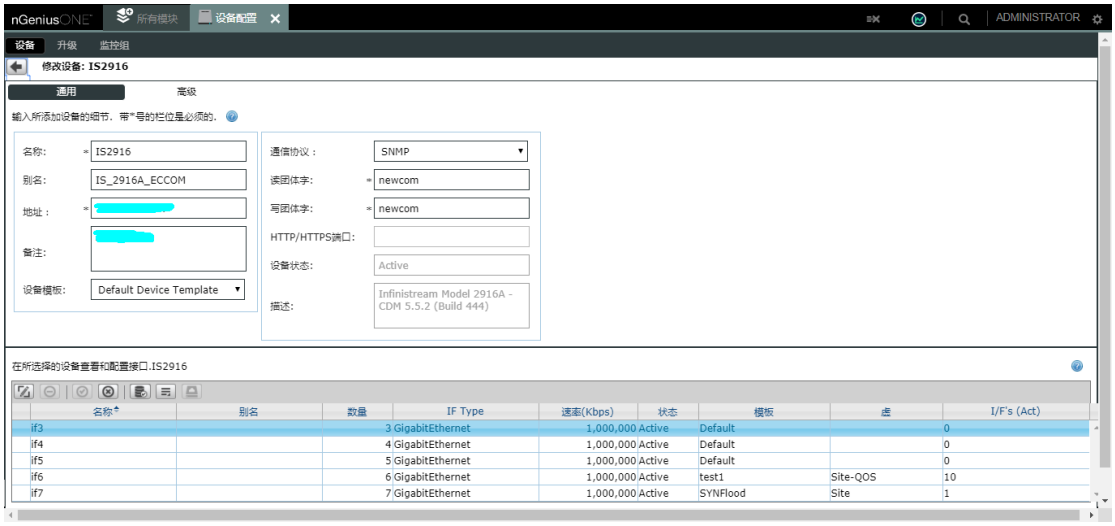




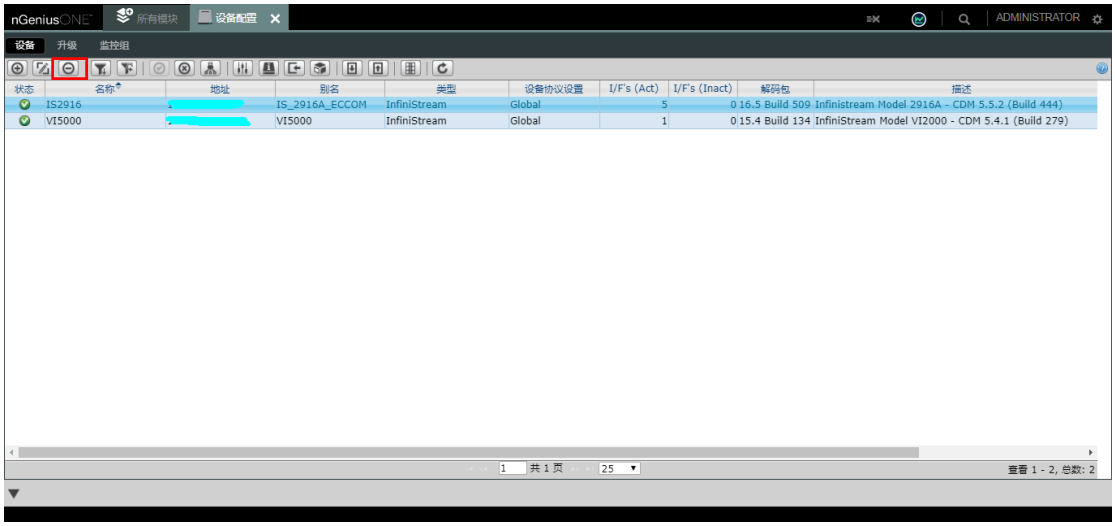
添加探针后可以对探针进行以下操作：

①  ，可以查看或修改该探针的名称、IP 地址以及接口名称等信息；

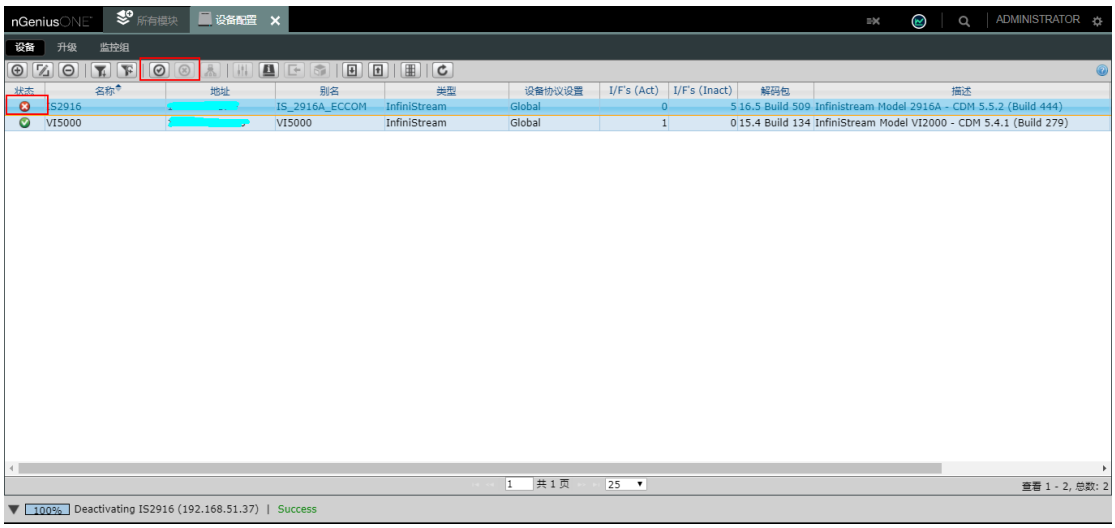




②  ，可以删除探针；

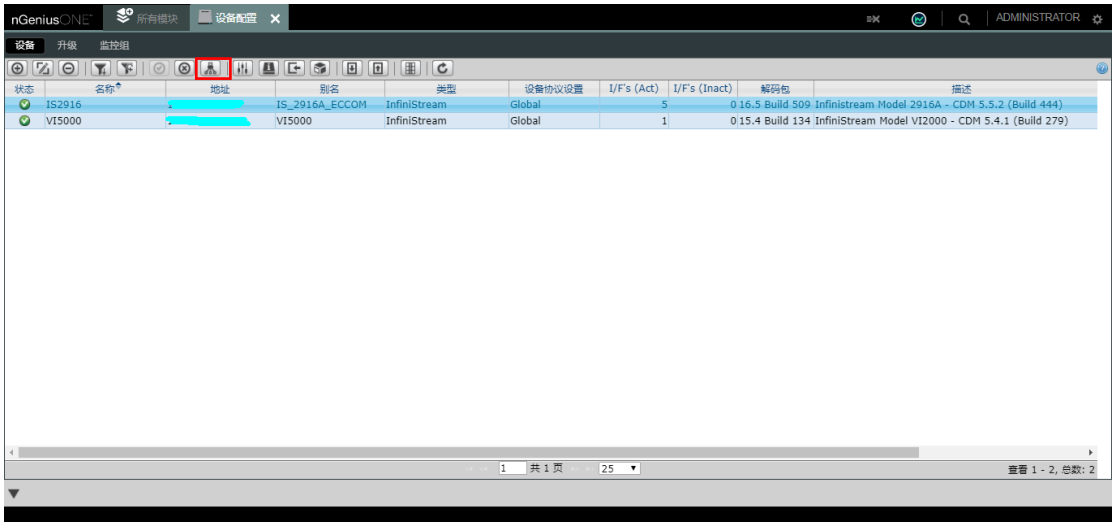


③  /  ，可以将探针禁用/激活；

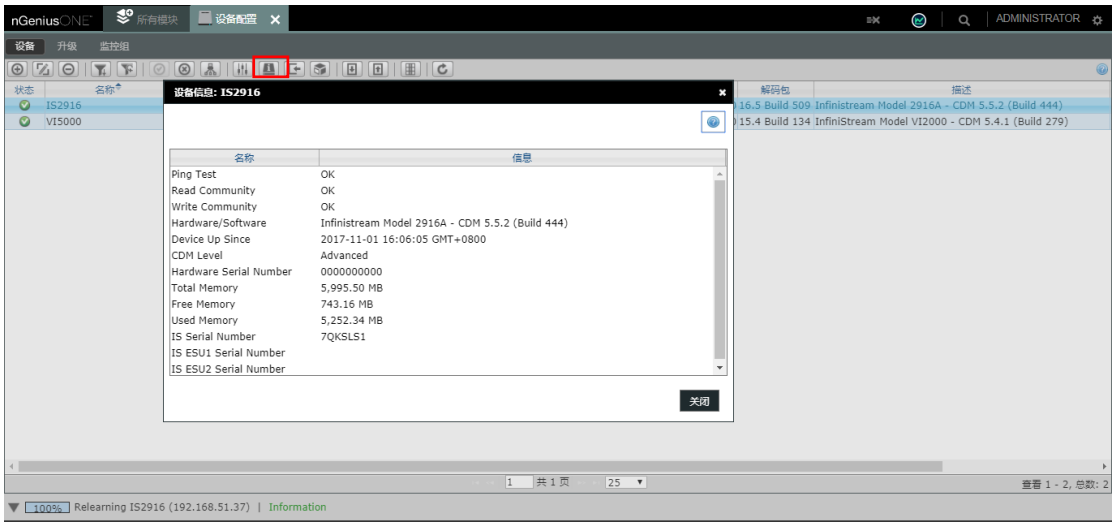


④  ，可以将 nGeniusONE 上添加的应用定义、Site 等配置同步到探针上，此项是为了

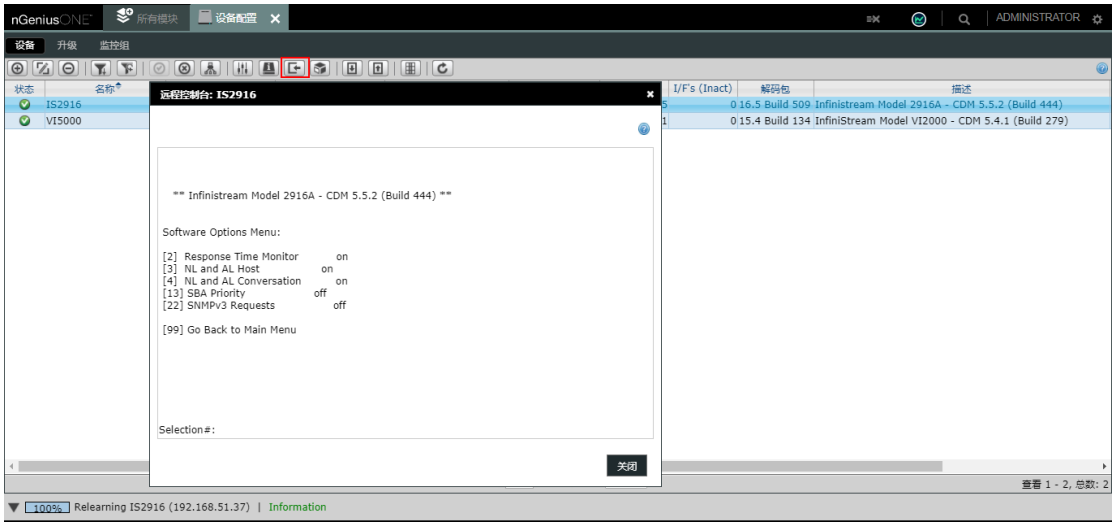
加速同步，一般 5 分钟内自动同步；



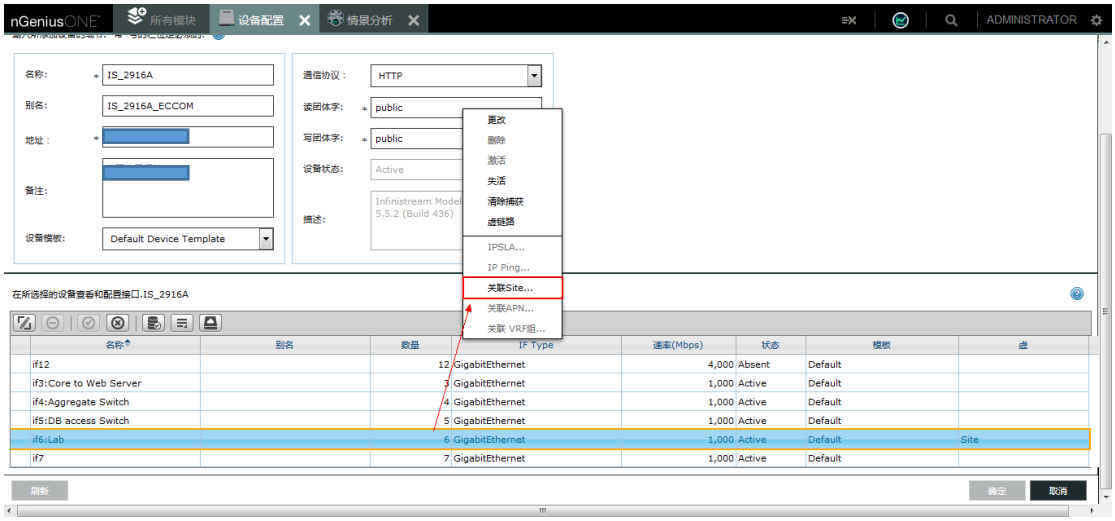
④  ，可以查看该探针的硬件信息包括型号、序列号以及内存使用情况等；



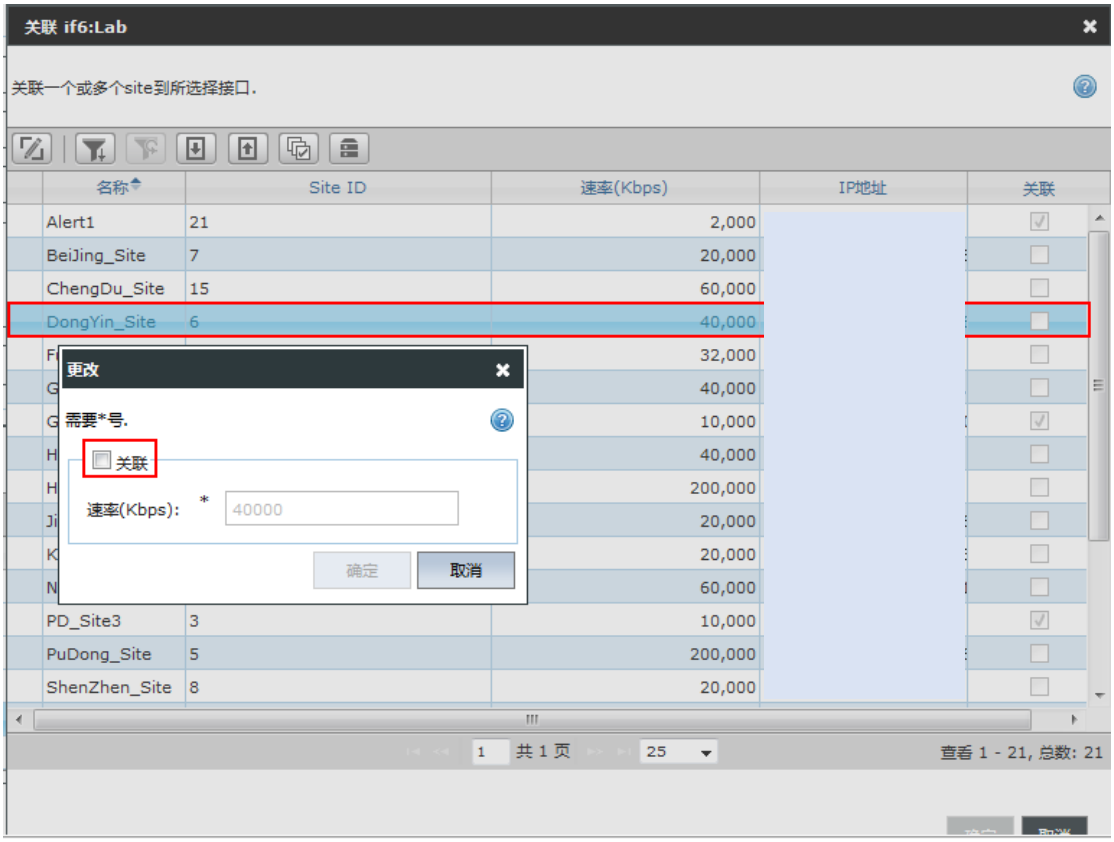
⑤  ，远程登录，可以进入该探针的命令行配置界面；



⑥ 关联 site，进入到探针详细信息，右键点击探针接口，选择“关联 site”



双击需要被关联的 site，勾选“关联”选框



4.2 配置应用

4.2.1 添加自定义应用

对于非标准的应用，例如用户自己开发的或者未运行在标准端口上的标准应用，需要在 nGeniusONE 服务器中进行预先定义，才能正确的被工作台呈现；

管理自定义应用需在“全局设置”里面操作。

（注：全局配置功能是 nGeniusONE 系统中极其重要的管理功能，可定义用户经常用到的功能，例如，增加新的协议或应用、增加新的主机组或子网 Site）；

此外，还有一个概念“应用组”，它是对同一类型的应用进行归组管理。

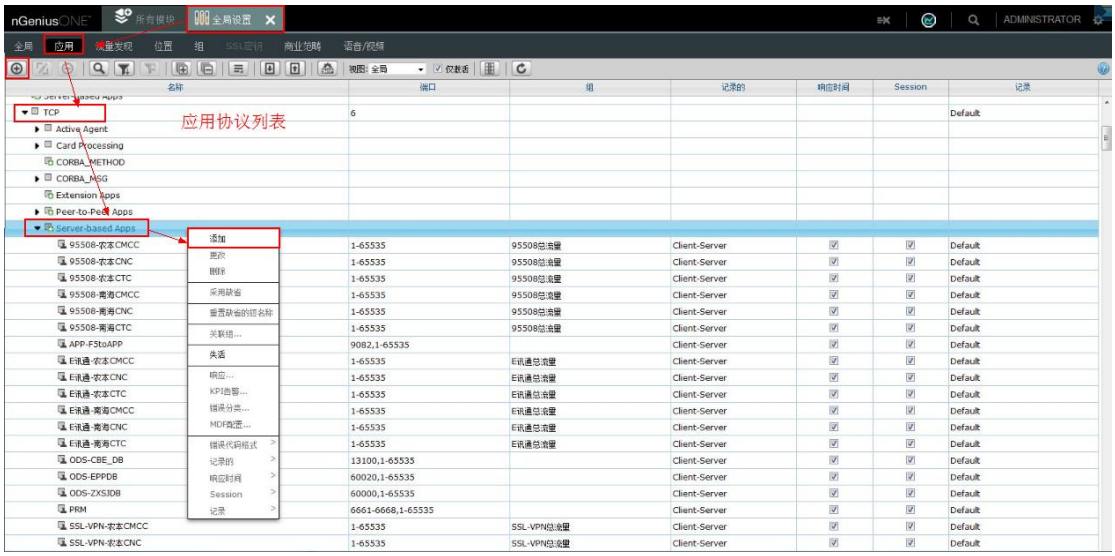
1） 添加自定义应用

下面的例子假设是对某种基于 TCP 的应用进行自定义添加，该应用名称是“CRM”，服务器的 IP 地址是 192.168.1.50 和 192.168.1.51，应用的端口号是 TCP 9008，我们将该应用归纳到“CRM 组”这个应用组中。

具体操作如下：

① 在应用协议目录中添加应用协议

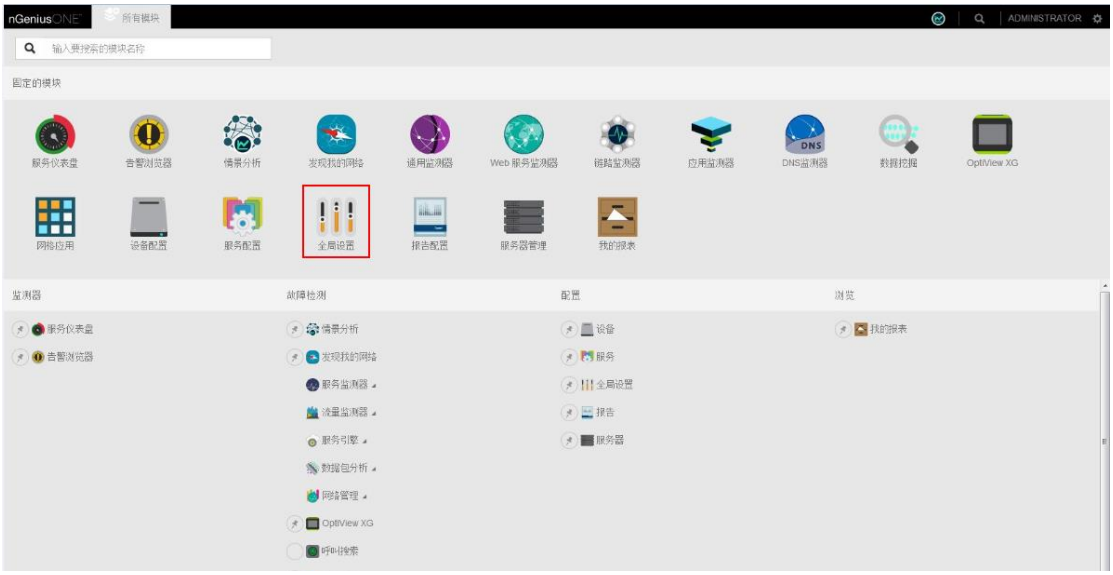
在“全局设置”→“应用”中，选择 TCP→Server-based Apps，然后点击左上方的  ，或者右键点击 Server-base Apps，选中 “添加”，如下图所示；



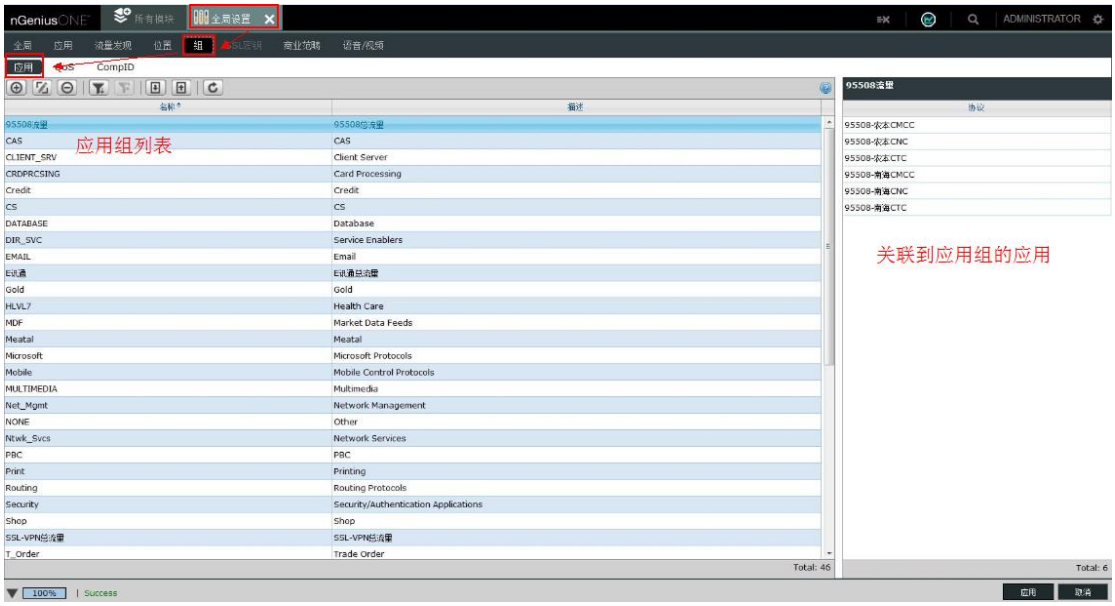
在弹出的添加界面里，应用类型选择“Server-based Application” ，输入应用短名称“CRM”，长名称“客户关系管理”，服务器的端口号“9008”，选择应用组为“客户关系管理”，在服务器 IP 地址栏中输入“192.168.1.50/32 和 192.168.1.51/32”。然后点击确认即可。

2) 添加应用组

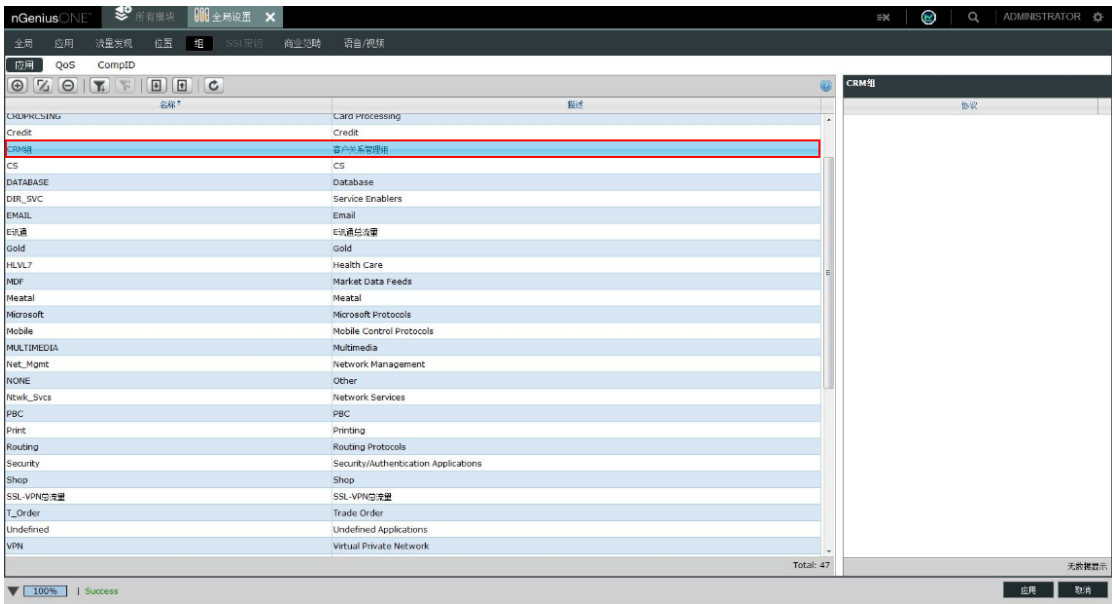
打开“所有模块”→“全局设置”，如下图所示:



点击全局设置中的第一个标签“组”→“应用”，如下图所示:

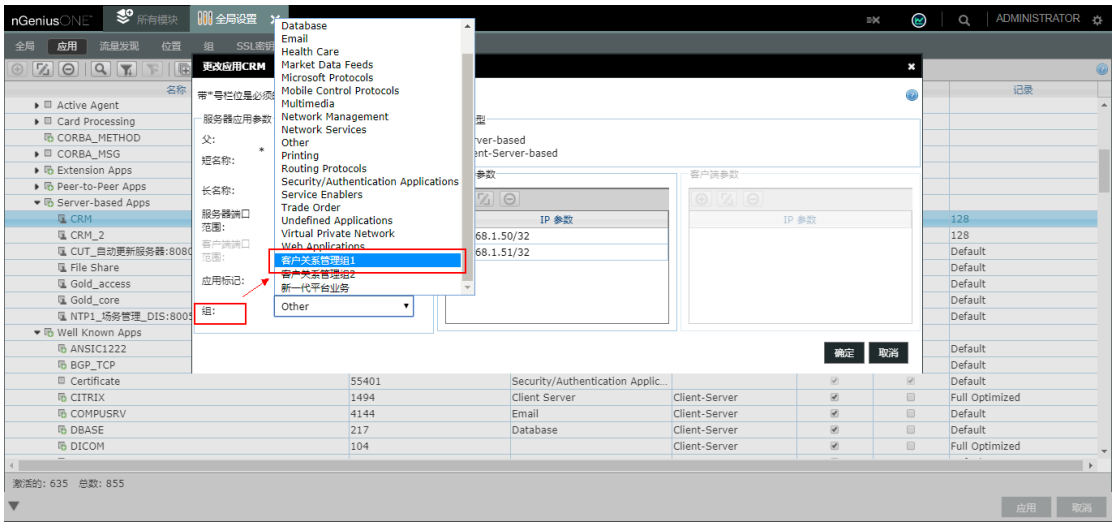


点击  添加应用组，在名称中输入“CRM 组”，在描述中输入“客户关系管理组”，点击确认即可完成新应用组的添加；



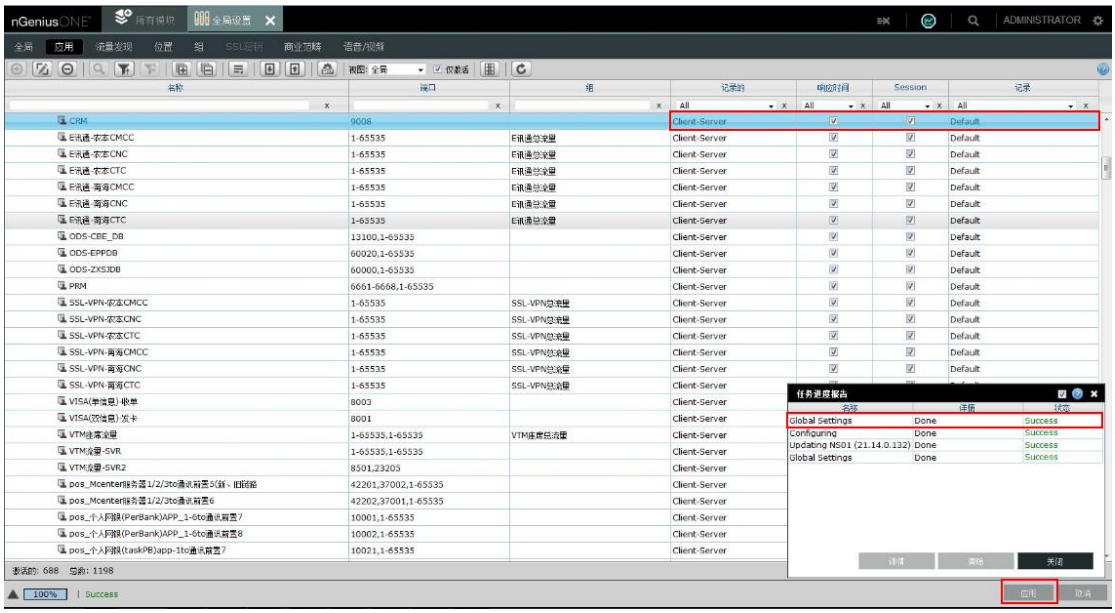
3） 将应用添加至应用组

在在“全局设置”→“应用”中，找到需要添加到应用组中的应用，双击该应用对其信息进行修改。在“组”的下拉菜单中选中对应的应用组后，点击“确定”

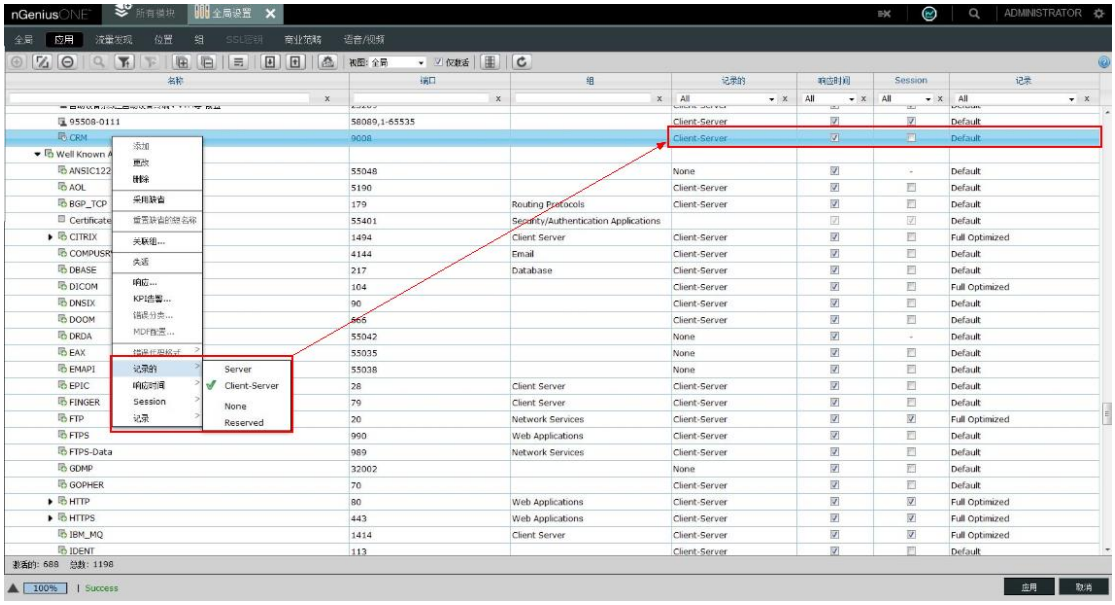


4.2.2 选择对自定义应用的监控内容

① 对于每个应用协议，可选择监控记录的内容，包括此协议的服务器、通信对和响应时间，以及定义该应用在探针上记录的包头大小（Default 缺省是记录包头 128 字节）。在相应的栏目中打勾，如下图所示：



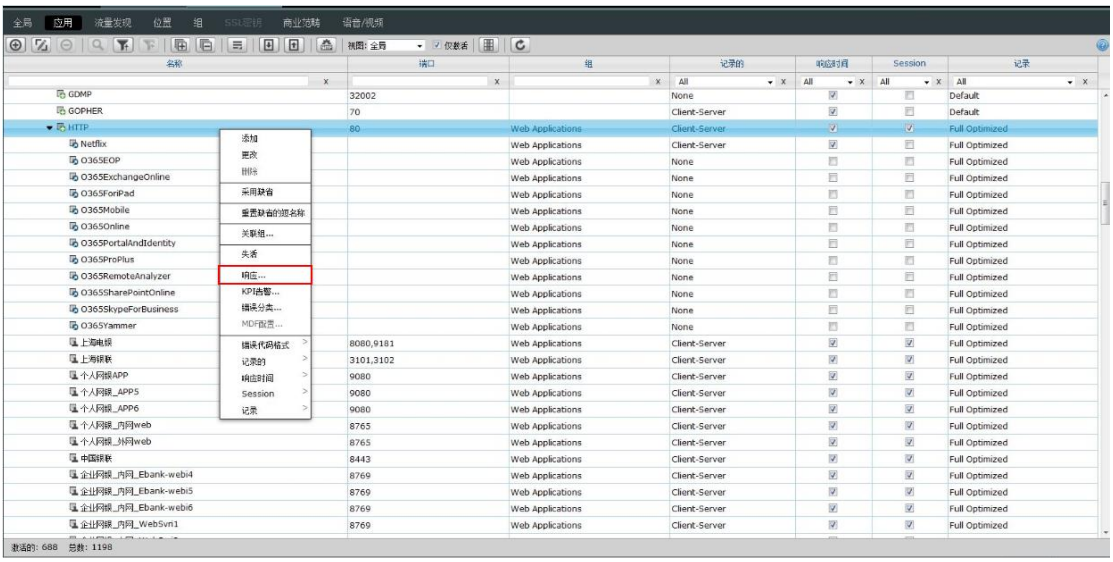
也可以通过右键点击应用，来进行配置



② 定义应用响应时间参数

应用的响应时间的分布区间的阀值是可以自定义的；

进入全局配置界面，然后右键点击你需要定义响应时间的应用，选择“响应”



编辑 5 个阀值，这些阀值会把该应用的响应时间分为 6 个等级：

注意可用性这一栏的大小，在 nGeniusONE 中，如果响应时间超过这个值，就认为是 Timeout（超时），就不会再去计算其大小，统一以该值来呈现。

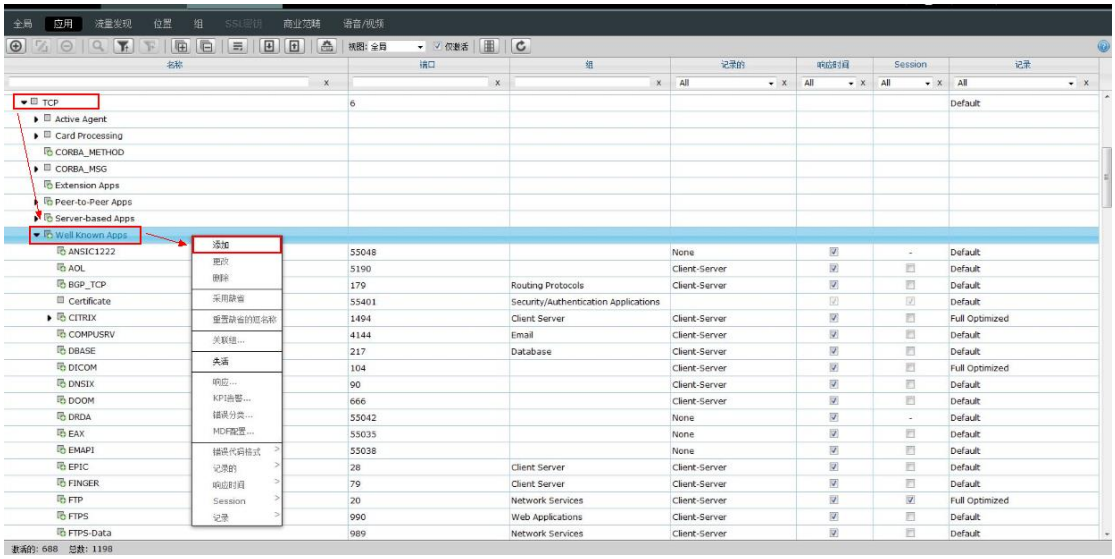
以上即可完成CRM应用的自定义，完成后，请在全局设置中点击“应用”来完成定义过程。

4.2.3 多种定义应用的方式

应用协议的定义，可选择 TCP 或 UDP 分别定义相应的协议，在 Well-known Apps 中定义单一端口的应用协议，在 Server-based Apps 中定义多端口或基于服务器地址的应用协议，在HTTP中可根据URL定义不同的应用协议。下面介绍如何添加不同的方式的自定义应用：

① 根据端口定义应用

在全局设置的“应用协议目录”中，根据需要定义的应用属于 TCP 还是 UDP，选择相应的 Well Known Apps，右键点击“添加”：

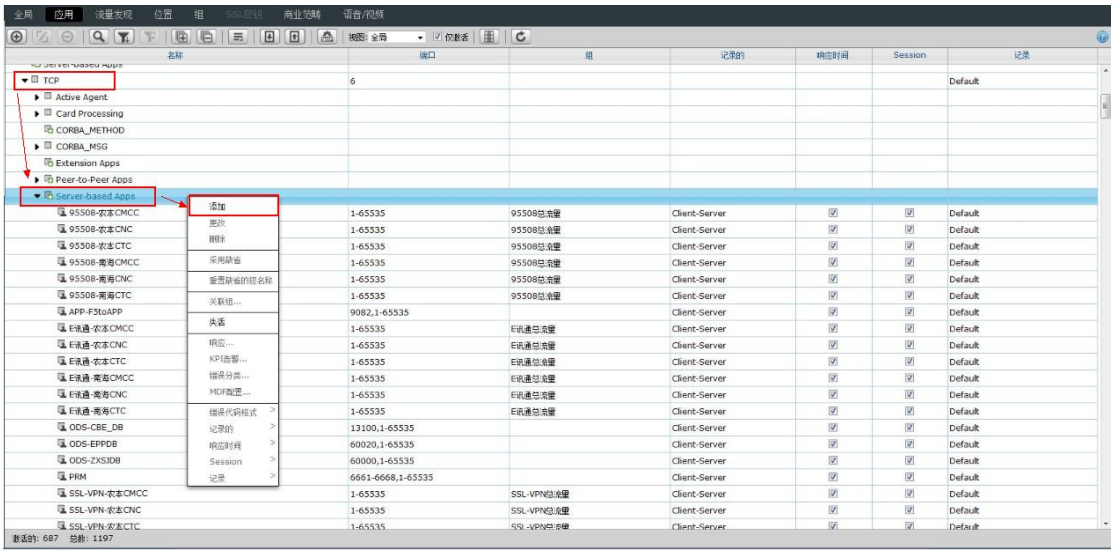


在弹出的窗口中填入应用短名称，应用长名称，端口号，附加端口号，所属应用组；

（附加端口号用于多端口的应用）

② 根据服务器 IP 地址和端口定义应用

在全局设置的“协议目录”中，根据需要定义的应用属于 TCP 还是 UDP，选择相应的 Server Based Apps，右键点击“添加”：

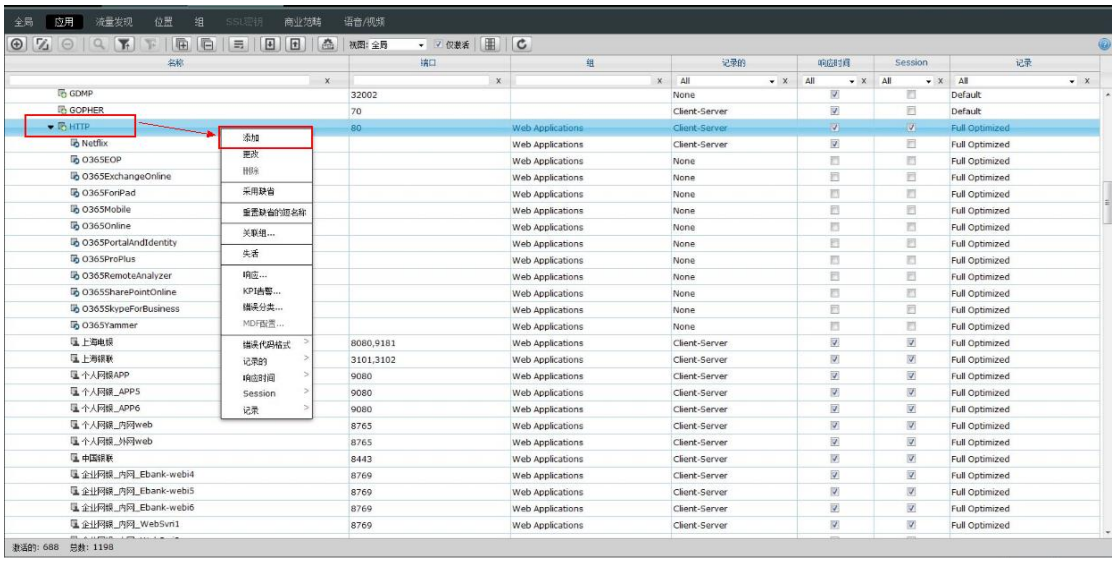


在弹出窗口中填入短名称，长名称，端口号范围，应用组，主机 IP 地址。

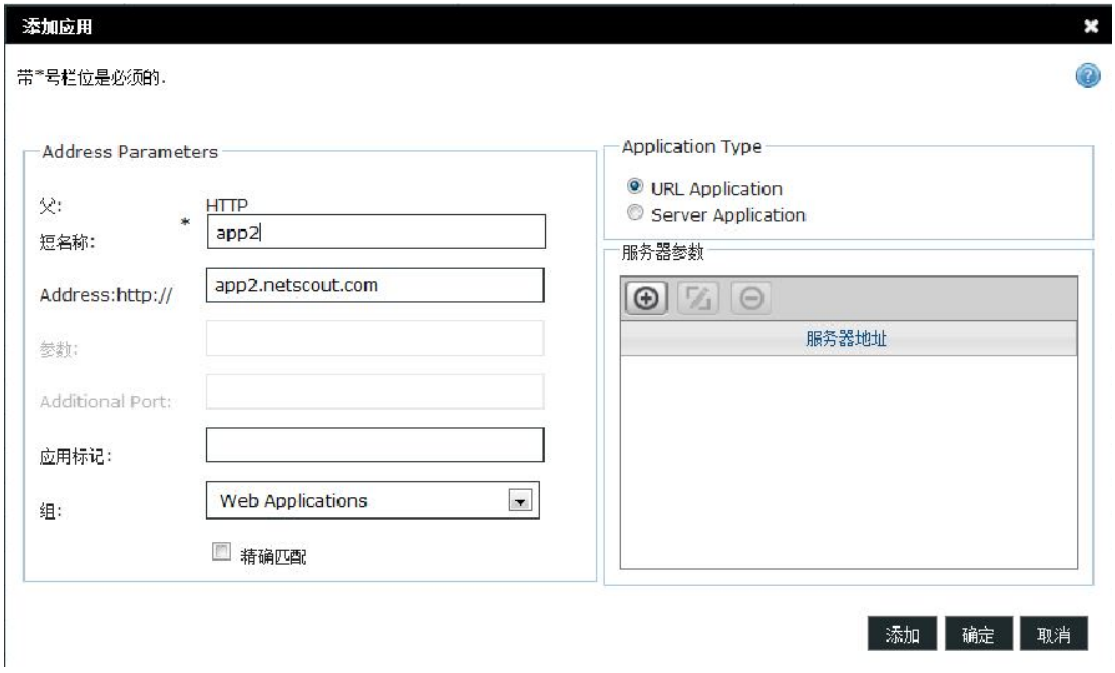
③ 根据 URL 定义应用

NETSCOUT 探针的 CRT 功能可用来分析特定 URL 应用协议。例如，用户的业务应用系统采用 URL，可按 URL 定义此应用。

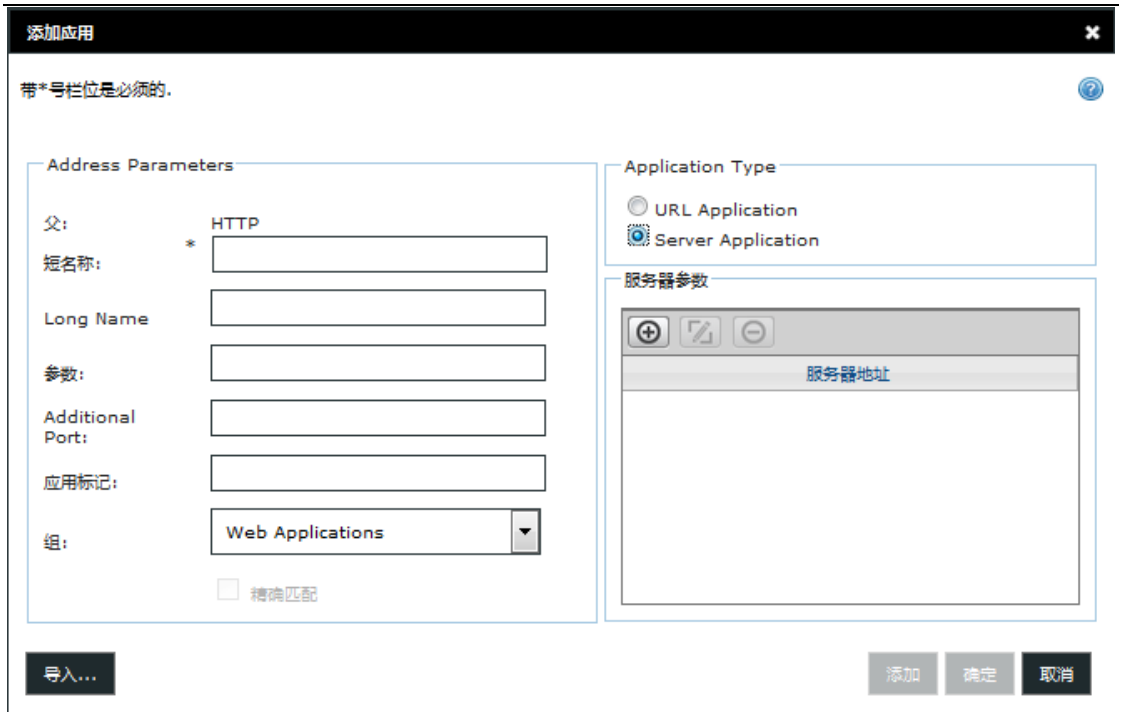
在 Well Known Apps 里找到 HTTP，右键点击“添加”，



在弹出窗口中填入 URL，应用短名称，选择应用组。



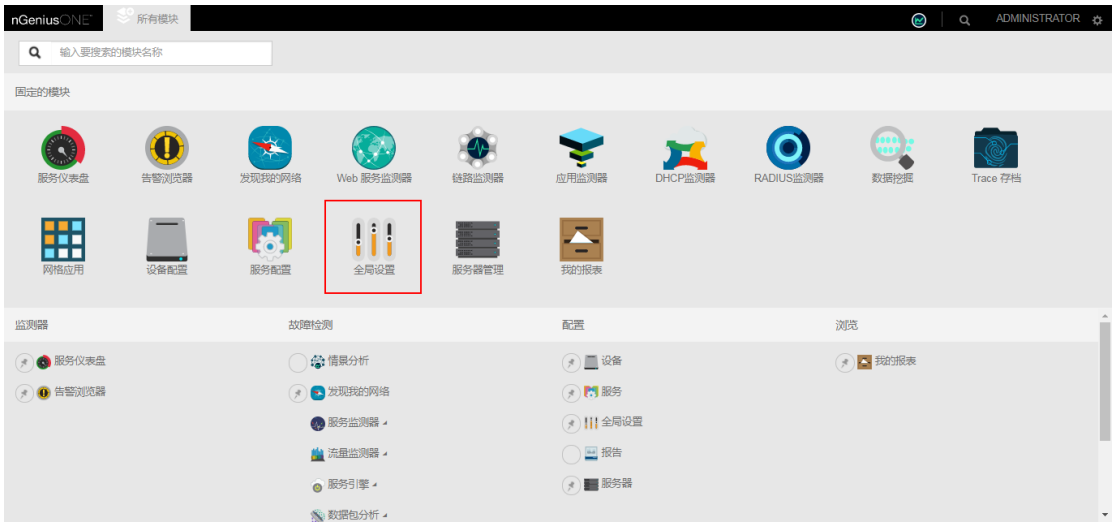
若点选 Server Application，则定义方式与②类似，在弹出窗口中填入短名称，长名称，端口号范围，应用组，主机 IP 地址。



若不选择“精确匹配”，则分析该 URL 及其下属子 URL。

4.3 配置全局设置

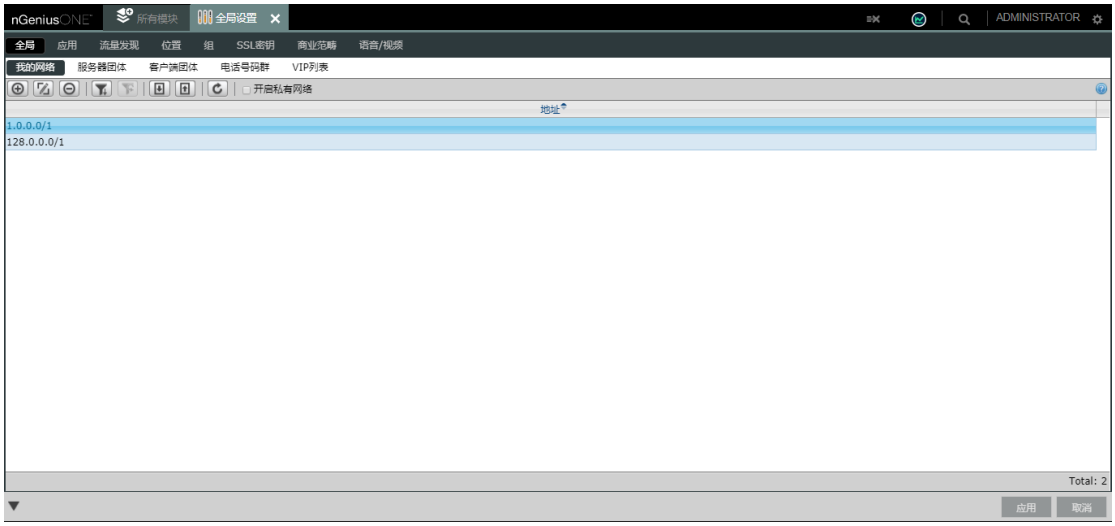
在“所有模块”界面中，选择“全局设置”



4.3.1 配置我的网络

在 nGeniusONE 中，“我的网络”是强制设置的，可以让 Infinistream 最小化数据表（注：我的网络中需要添加所有监控的 IP 地址段，nGeniusONE 只对包含在“我的网络”中的 IP 地址启用 ASI 统计功能，未包含的 IP 地址将不启用 ASI 统计功能，以减少不必要的数据噪音和数据分析量）。

在全局设置的“我的网络”界面中添加或修改需要监控的网段地址



⊕	创建一个我的网络定义
⊖	删除我的网络定义
	修改我的网络定义
/	显示/隐藏过滤器，对我的网络列表进行搜索
	重置过滤器
/	导入/导出我的网络定义
	刷新我的网络列表
Enable Private Network	选择该项可以添加“私有网络地址”

4.3.2 配置服务器和客户端团体

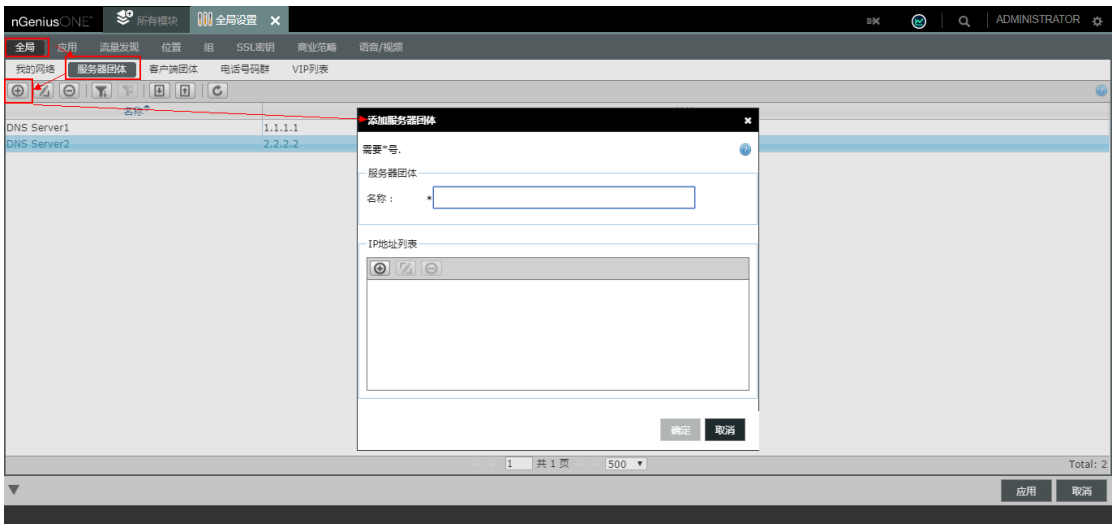
客户端团体和服务器团体是通过将客户端和服务器进行归类以减少分析数据量，并以群体的维度来分析具有某类相同性质的客户端或服务器；同时，也可以单独为某个服务器或客户端定义一个团体，在分析时以更友好的名称来显示，而不是显示IP地址。

服务器团体举例：企业的DNS服务器可能有多台，可以将所有DNS服务器都定义到“DNS服务器”团体中，在分析时可从DNS服务器群体的维度进行数据汇总。

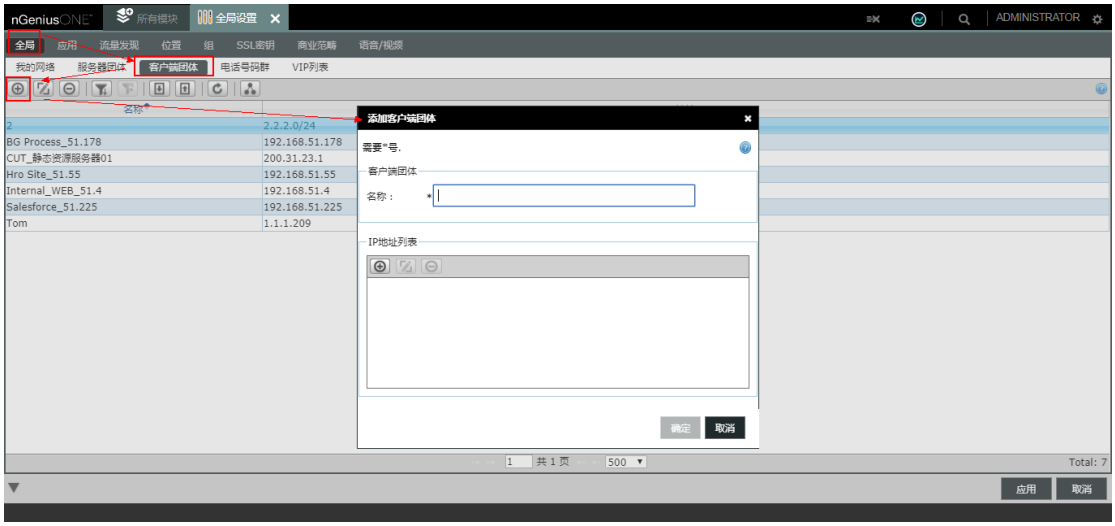
客户端团体举例：企业可能有多个分支机构或部门，可以以IP地址范围来区分，则通过定义客户端团体，在分析时就可从客户端群体的维度进行数据汇总。

（注：要在服务器/客户端团体中设置 IP 地址，这些 IP 地址要包含在“我的网络”）

在全局设置的“服务器团体”界面中添加或修改相应的服务器地址，如下图：



在全局设置的“客户端团体”界面中添加或修改相应的客户端地址，如下图：



4.4 服务配置

nGeniusONE 是以服务为中心的工作流程，因此如果要在 Dashboard 中展示服务性能，需要事先定义服务域和服务。

为了更好的展示服务，nGeniusONE 提供按域的方式组织排列服务，可按多种方式组合创建服务域：

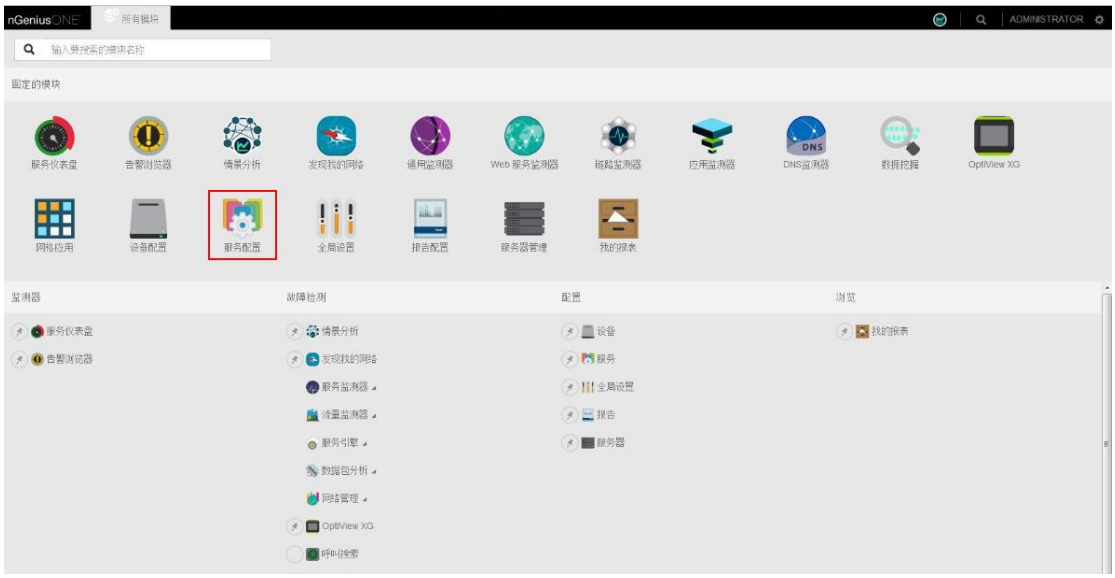
- 地理位置
- 业务
- 功能部门
- 分支机构

例如下图所示：

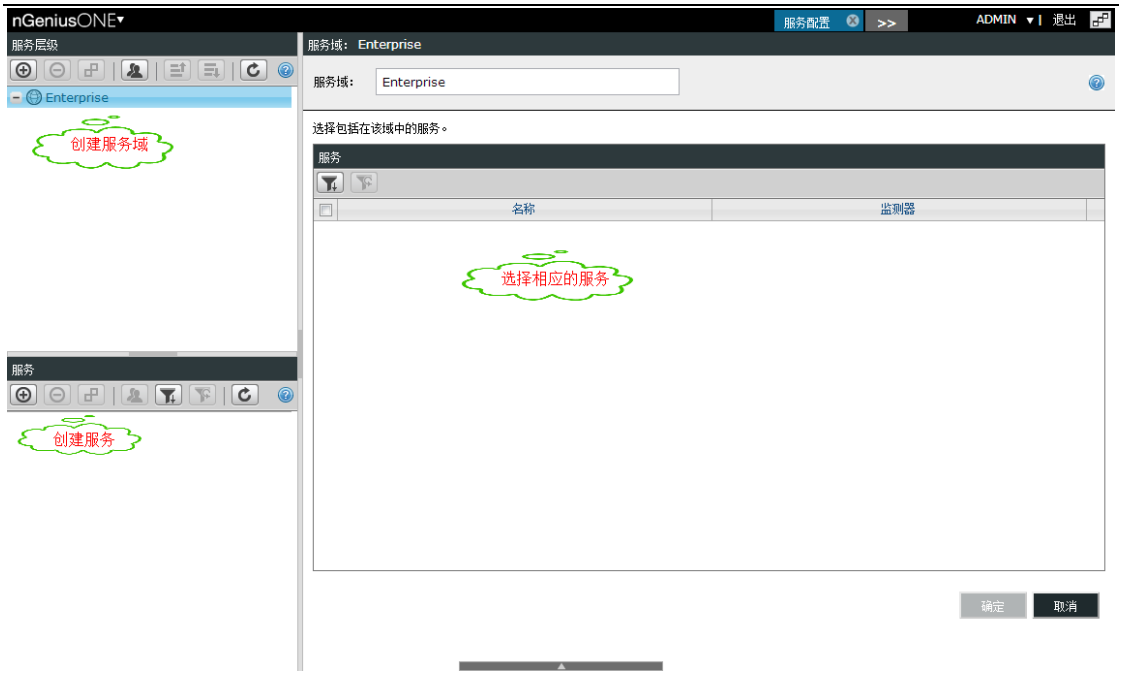
使用“服务配置”去定义您想要在 nGeniusONE 中监控的服务域和服务。

4.4.1 创建新的服务域

在“所有模块”界面中，选择“服务配置”，如图；



将会出现如下图所示的服务配置的界面，如图；



图标解释

	代表一个未分配的服务
	代表一个已分配的服务
	代表一个未分配的服务域
	代表一个已分配的服务域

	创建一个新的服务域或服务
	删除一个服务域或服务
	在同一个位置创建一个已存在服务域的副本
	分配所选中的服务或域给用户或组
	对服务或域重新排序，上升或下降
	刷新服务层级

在服务层级中创建一个新的服务域，或修改缺省的 Enterprise 服务域。服务域可以多级嵌套，最大支持 8 个级别。

如下图所示，创建一个“NETSCOUT 北京”的服务域：

4.4.2 创建新的服务

服务包含两个主要元素：一个或多个应用，一个或多个探针接口（或虚接口）。另外，可以针对每个服务配置告警档案。

在服务中创建新的服务或修改已定义过的服务。

在服务中选择  ，即可出现如下图所示的服务配置界面：

在“服务成员”中选择  添加服务要素（应用+探针接口），如下图所示：

4.5 配置服务告警

4.5.1 理解服务告警

当配置了服务告警，能够针对应用、服务器、语音服务或网络的问题产生主动的智能警报。

告警分为以下三种类型：

A.基线告警

- 超过统计学衍生基线而产生的告警
- 基线是基于分析每个服务成员进行计算，并持续根据当前行为进行调整。可以通过“配置基线例外”来排除特定时间段不计算基线
- 基线基于周期性或非周期性数据
- 当支持的量度指标高于基线时将自动产生告警，当前版本支持的量度指标包括：交易率(Transaction Rate)，失败率(Failure Rate)，服务器和客户端重传百分比(Server and

Client Retransmission Percentage)，平均响应时间(Average Response Time)

B.基于阀值的告警

- 比较当前数据和用户自定义的阀值，包括上升或下降阀值
- 阀值可以设置警告和关键（Warning and Critical）两个级别
- 当支持的量度指标高于或低于阀值时将自动产生告警，当前版本支持的量度指标包括：交易率，失败率，重传百分比，平均响应时间，进/出抖动问题的百分比 （percentage of problematic Jitter (Ingress/Egress)），进/出 MOS 问题的百分比（percentage of problematic MOS（Ingress/Egress)），进/出丢包问题的百分比（percentage of problematic Packet Loss (Ingress/Egress)）

C.可用性告警

- 针对一个位置（Location）的不可用状态产生告警
- 基于位置的可用性告警适用于包含位置定位（Location Key）的服务。当一个服务成员没有交易（Transaction）时将触发交易位置告警，当服务成员没有流量（Traffic：观察到的总比特率）时将触发流量位置告警

基于服务的告警需要考虑以下因素：

A.缺省将不产生告警；需要事先启用和配置服务的告警。

B.在在新安装的环境，统计基线需要学习一定时间的数据：

- 可用性告警需要学习 1 天的数据
- 非周期性基线告警需要学习 3 天的数据
- 周期性基线告警需要学习 1 周的数据

C.基于服务的告警（Service-Based Alert）是通过告警档案（Alert Profile）来管理的，每个服务可以关联一个缺省或自定义的告警档案。一个告警档案可以包含一个或多个触发器

（Trigger），每个告警档案最多可以有 10 个触发器。缺省的告警档案可以修改但不能删除。

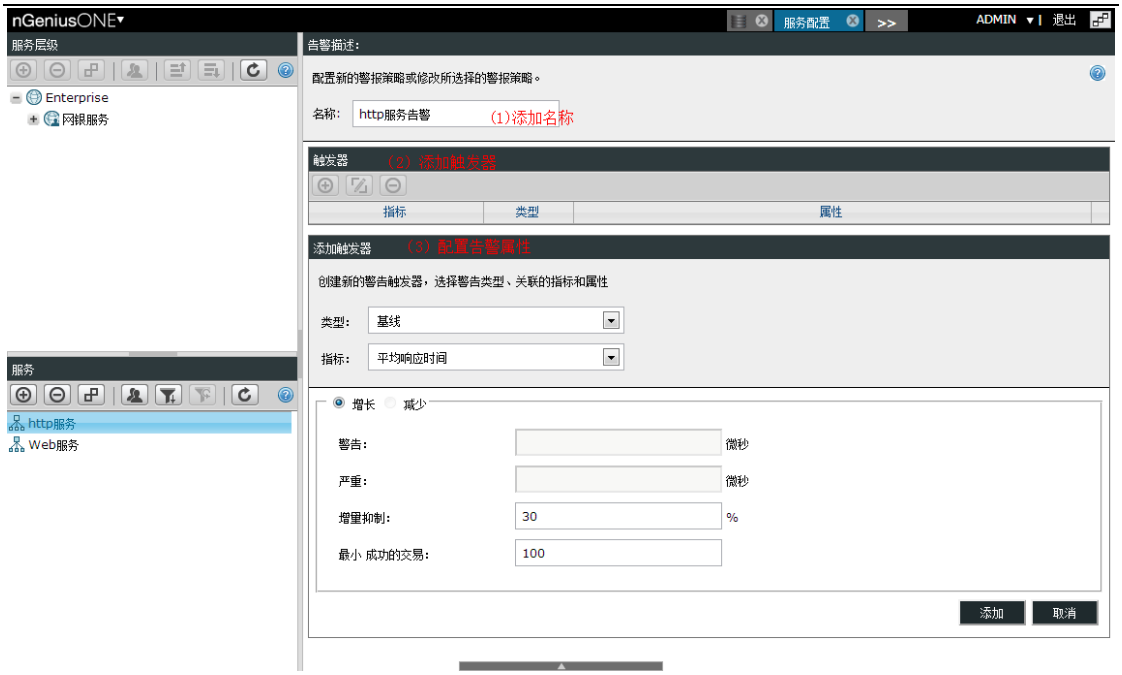
4.5.2 告警档案

在告警档案（Alert Profile）面板中可以查看、配置和修改每个告警档案以及相关的触发器（Trigger）。

告警档案的配置：选择需要修改的服务→勾选“警报”→在“简况”中选择已有的告警档案或添加新的告警档案。

点击“ ⊕ ”，可以添加新的告警档案，

（1）添加告警档案的名称（2）添加触发器（3）配置告警属性，如下图所示：



告警触发器包括基线和阀值两种。

4.5.3 触发器

触发器设置	项目	描述
类型（Type）	基线(Baseline)	测量基于统计方法的基线
	阀值(Threshold)	比较用户自定义的阀值（上升或下降）
	可用性(Availability)	基于位置（Location）的交易（Transaction）或基于位置的流量的可用性
指标（Metric）	基线指标	交易率（Transaction） 失败率（Failure Rate） 重传百分比（Retransmission Percentage） 平均响应时间（Average Response Time）
	阀值指标	交易率，失败率，重传百分比，平均响应时间，进/出抖动问题的百分比 （percentage of problematic Jitter (Ingress/Egress)），进/出 MOS 问题的百分比（percentage of problematic MOS (Ingress/Egress)），进/出丢包问题的百分比（percentage of

		problematic Packet Loss (Ingress/Egress))
	可用性指标	基于位置的交易率（Transaction rate-Location）(Transaction) 基于位置的总比特率（Total bit rate-Location）(Traffic))
属性（Attributes）	增长或减少（Increasing/Decreasing）	基线或阀值的方向
	警告级别(Warning Alert)	设置达到警告级别的百分比或值
	严重级别(Critical Alert)	设置达到严重级别的百分比或值
	增量抑制 (Delta Suppression)	只针对基线告警有效。在采样期间的最大值和历史数据的中间值之间可允许的百分比差异，如果当前数据的最大值小于指定的百分比，将不产生告警。
	最小值(Minimum)	低于交易率、数据包或流（Stream）的最小值，将产生告警

5. 帐号管理

帐号权限设置是用于给系统管理员加强 nGeniusONE 系统的安全性的一种辅助工具；通过给一个用户帐号分配一个或多个角色，可以控制用户使用系统特定的功能。用户帐号管理具备灵活和安全性，可以通过增加或删除权限、创建自定义的角色、分配用户到某个组和给用户添加约束等来修改预定义的角色。我们可以通过本地或第三方机制进行验证和授权用户权限。

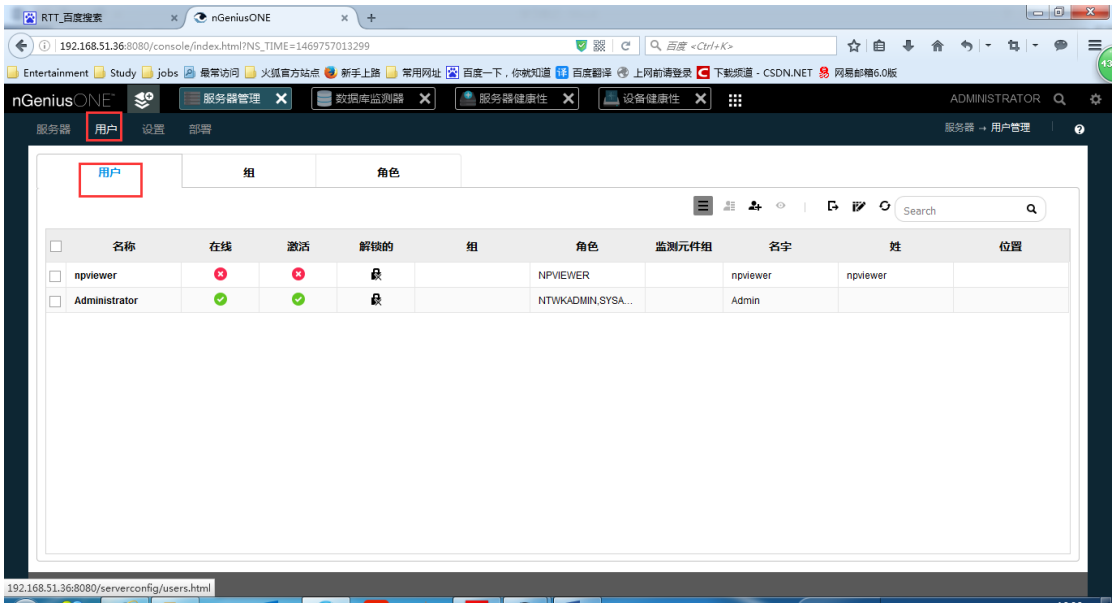
系统默认创建一个默认帐号 npviewer，用于提供给那些不具备修改 nGeniusONE 系统权限的用户进行使用报表功能（只读），另外还有一个默认帐号是 Administrator，该帐号包括 System Administrator 和 Network Administrator 角色，因为 System Administrator 的权限可以控制用户和角色，所以至少要有一个用户帐号必须分配 System Administrator 角色权限。

注:最大并发用户数为 55 个,其中包括 5 个具备 SYSADMIN 权限和 50 个 non-SYSADMIN 权限。

5.1 创建用户帐号的配置步骤

已经被分配到角色 System Administrator 的用户帐号可以创建用户帐号、分配用户角色、分配用户到组和限制用户访问数据等。

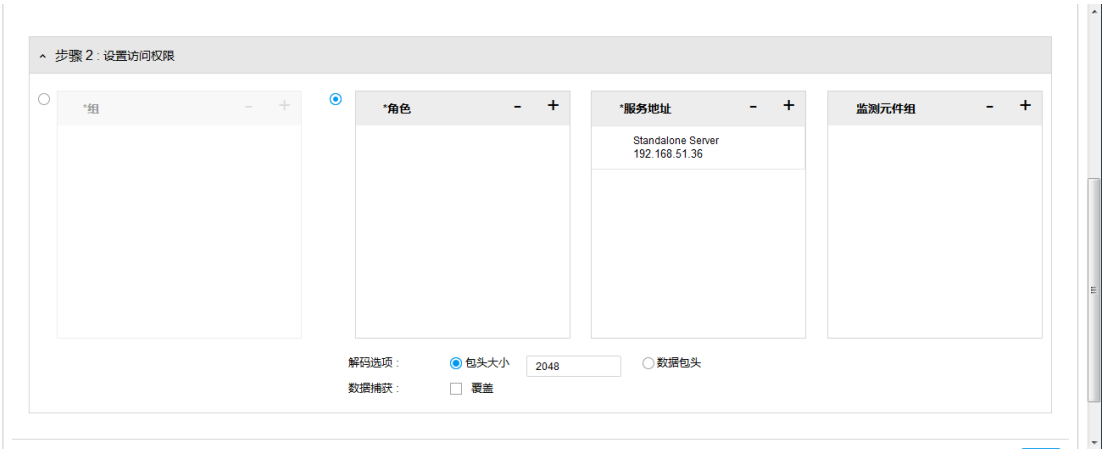
单击“配置管理器”→“服务器管理”图标，选择“用户”→“用户”，如图;



单击  添加用户，如图

根据提示输入相应信息，如用户名、密码、邮箱、位置和电话等，如图

根据需要配置组别、角色、服务器地址、解码选项、数据捕获和禁用帐号选项等来设置帐号权限，



完成以上配置后单击“确定”进行提交；

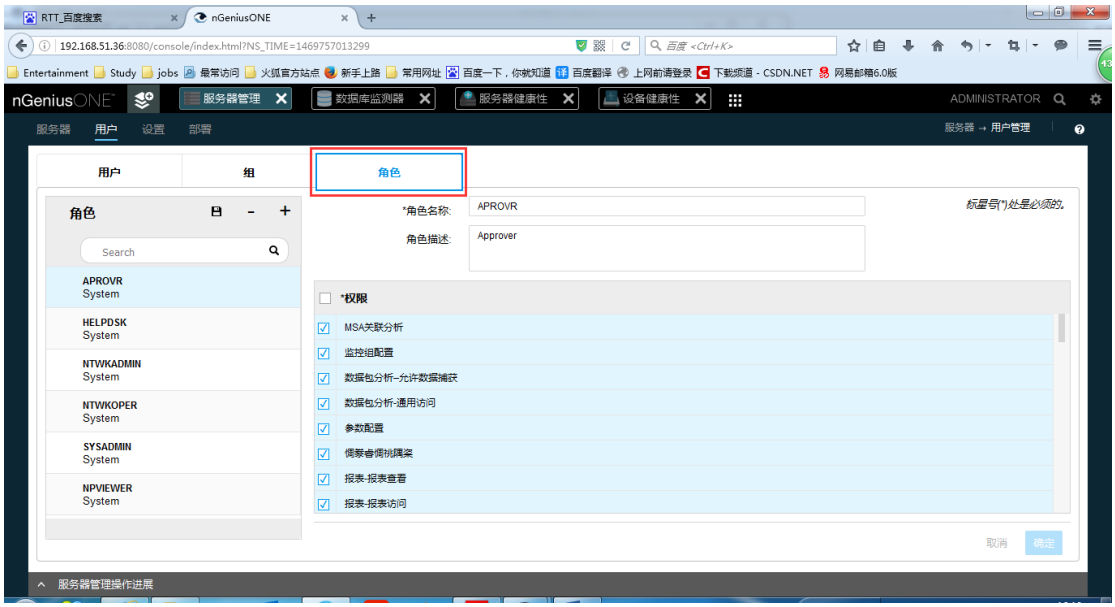
5.2 分配和创建用户角色

服务器管理模块提供了六个预定义的用户角色有效描述了 nGeniusONE 配置和维护任务，分别是 System Administrator、Network Administrator、Approver、Network Operator、Help Desk 和 NPVIEWER，这些帐号默认都已经分配了相关的系统功能或权限（详见附件 1）。这些系统角色不能被修改，但是我们可以通过创建自定义用户角色并根据需要分配权限。当我们设置自定义角色的权限后，所有分配到该角色的用户权限都将随之发生改变。另外，如果你想要修改某个特定的用户或组的权限而不影响所有共用该角色的用户，可以自定义一个用户角色来实现。例如，你想为一个用户修改 Help Desk 角色而非所有分配该角色的用户，则可以通过创建一个基于 Help Desk 角色并分配其他权限的自定义角色进行授权。

注：如果在设备配置运行过程中修改权限，不会有通知发送给设备用户，用户必须通过重新登录才使得设置生效。

5.2.1 基于已有角色分配和定义一个新用户角色配置步骤

单击“配置管理器”→“服务器管理”图标，选择“用户”→“角色”，如图；



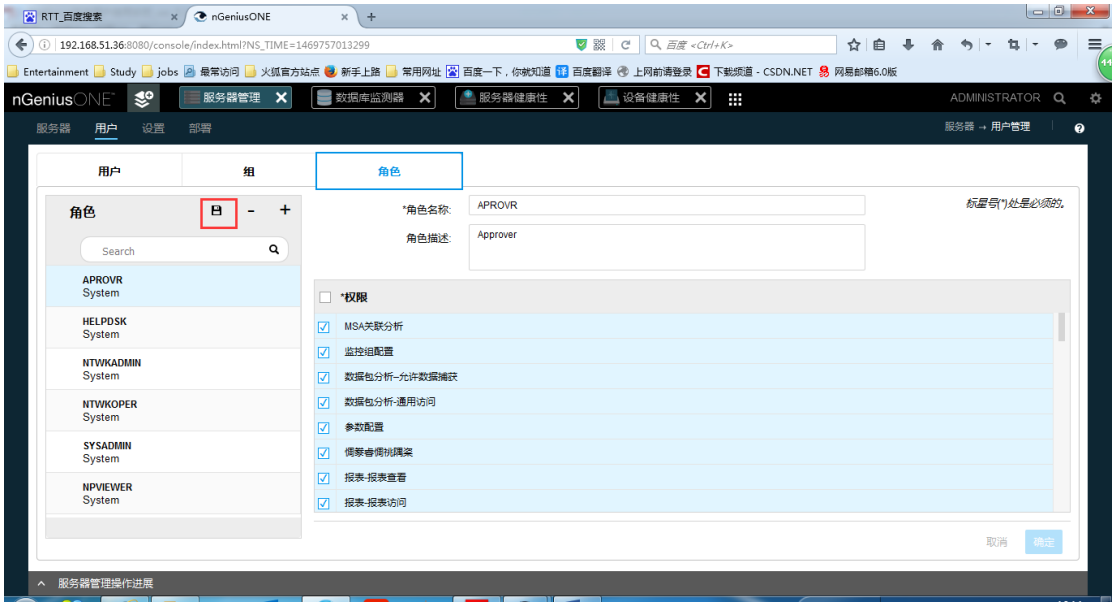
从角色面板选择预定义的角色查看当前分配的功能

系统默认定义的六个角色分别是 APROVR、HELPDSK、NTWKADMIN、NTWKOPER、SYSADMIN、NPVIEWER；系统默认已经定义了这六个角色分别所具备的权限，如有需要可以自己另行新建角色并赋予相应的权限，具体权限详见下表：

角色	功能	备注
npviewer	报表-报表查看、报表-报表访问	
NTWKOPER	数据包分析-通用访问、参数配置、报表-报表查看、报表-报表访问、报表-报表和报表模版配置、访问 SDM、用户账户自服务、View User Identity	
APPOVR	MSA 关联分析、监控组配置、数据包分析-通用访问、参数配置、报表-报表查看、访问、模版配置、访问 SDM、Session Analysis Deilldown、镜像配置、Subscriber Intelligence 关联分析、用户账户自服务、view user Identity	
HELPDSK	数据包分析-通用访问、参数配置、报表-报表查看、访问、模版配置、访问 SDM、用户账户自服务、view user Identity	

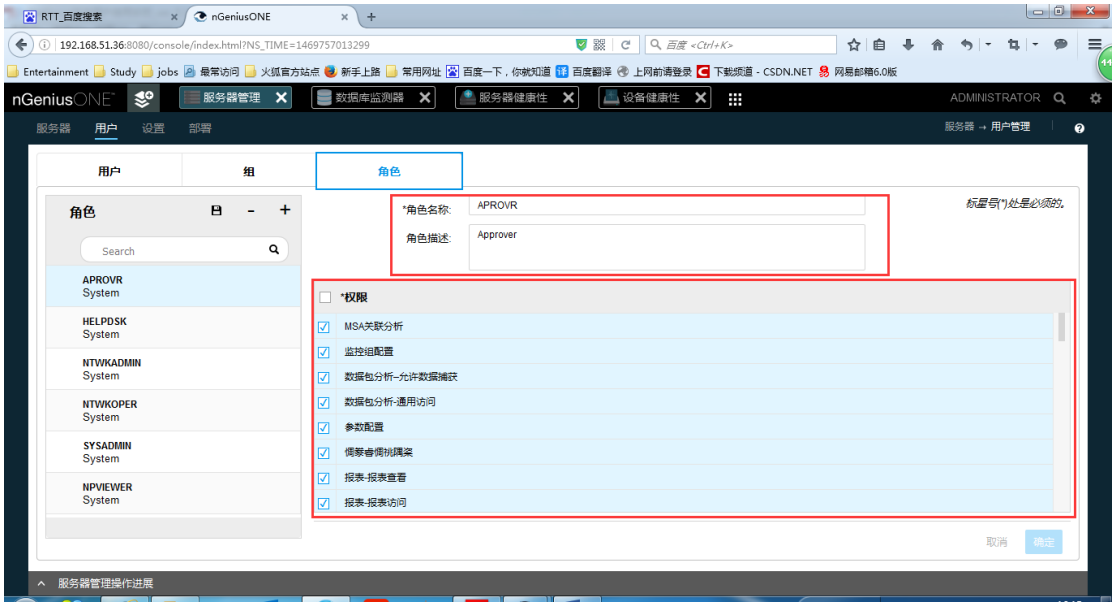
NTWKADMIN	Business Type Configuration、数据库配置（包括备份、压缩、清除）、设备配置、设备健康性查看、设备模版配置、载入 Enterprise Intelligence、排除配置、全局设置配置、MSA 关联分析、消息日志配置、监控组配置、数据包分析-数据捕获覆盖配置，专家数据挖掘规则配置，通用访问，HTTP 回话重组，媒体文件重放，回访配置，时间触发器配置，捕获文件输出和保存、参数配置、xx、报表创建、报表-报表查看，公共报表创建，报表访问，报表和报表模版配置、响应时间配置、服务器（分布式）-正在添加本地服务器、服务器处理远程控制台登录、服务配置、访问 SDM、服务访问控制、Session Analysis Drilldown、软件更新配置、Spaces Configuration、镜像配置、Subscriber Intelligence 关联分析、用户账户自服务、View User Identity、工作台颜色设置、工作台权限转换	
SYSADMIN	Business Type Configuration、数据库配置（包括备份、压缩、清除）、载入 Enterprise Intelligence、外部服务器认证配置、消息日志配置、消	
	息日志查看、nGenius 分析查看、参数配置、xx、报表管理、报表-报表查看，报表访问，报表和报表模版配置、服务器（分布式）-正在添加本地服务、服务器健康查看、服务器配置、访问 SDM、服务访问控制、软件更新配置、Spaces Configuration、用户账户自服务、用户组管理、用户角色管理、用户会话管理、用户账户管理、工作台颜色设置、工作台权限转换、nGenius 部署数据库配置、查看	

单击“复制”按钮，如图



给新建角色设置一个唯一的名称（不支持空格和特殊字符）并进行简要描述后选择或反选对

应的需要分配的权限的勾选框，如图



单击“确认”进行提交；

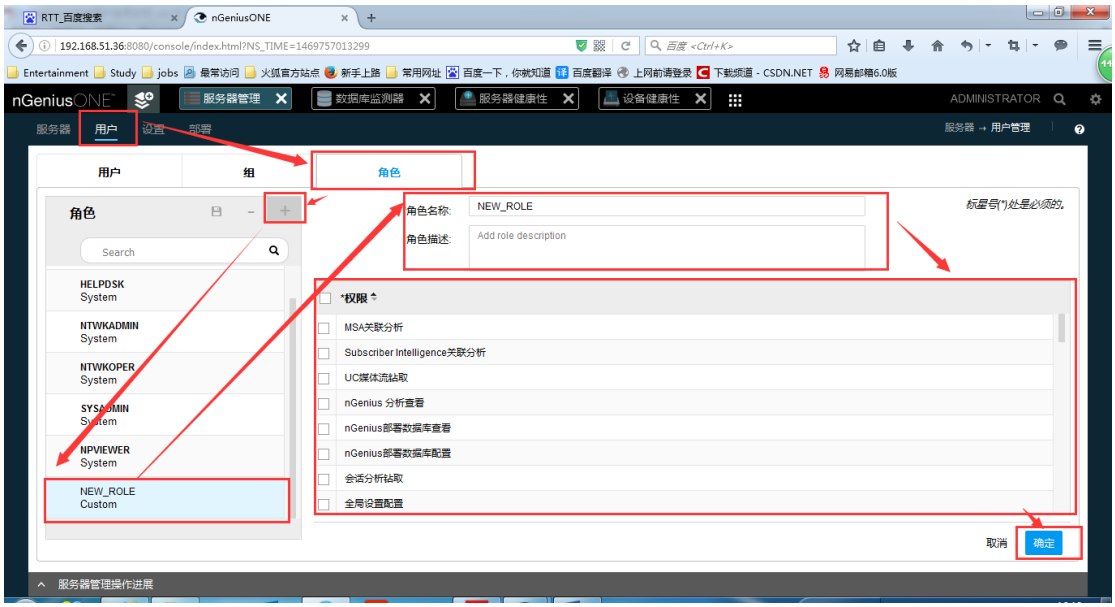
5.2.2 定义一个自定义的用户角色配置步骤

单击“配置管理器”→“服务器管理”图标，选择“用户”→角色

单击“添加角色”，输入一个唯一的角色名称（不支持空格和特殊字符）并进行描述

在权限界面勾选想要分配给这个角色的功能，至少需要为每一个角色分配一种权限；

单击“确认”进行提交；



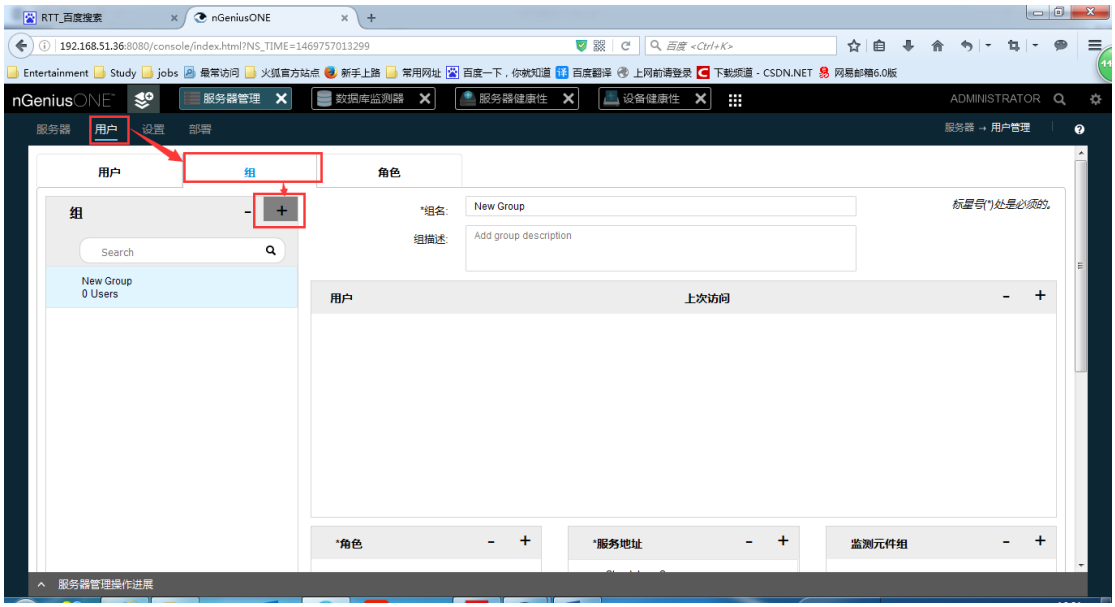
5.2.3 创建用户组步骤

为了有效管理多个账户，可以通过将这些帐号分配到一个组并为该组关联特定的权限，需要注意的是一个用户帐号只能分配到一个组且必须给该组至少分配一个用户角色，分配后用户的权限以组权限为准；例如用户 User1 本来分配了 System Administrator 角色，但此时将其添加到分配了 Help Desk 角色的组中，则 User1 从属的角色为 Help Desk 而不是 System Administrator。因此，在为组分配角色时需要小心谨慎。

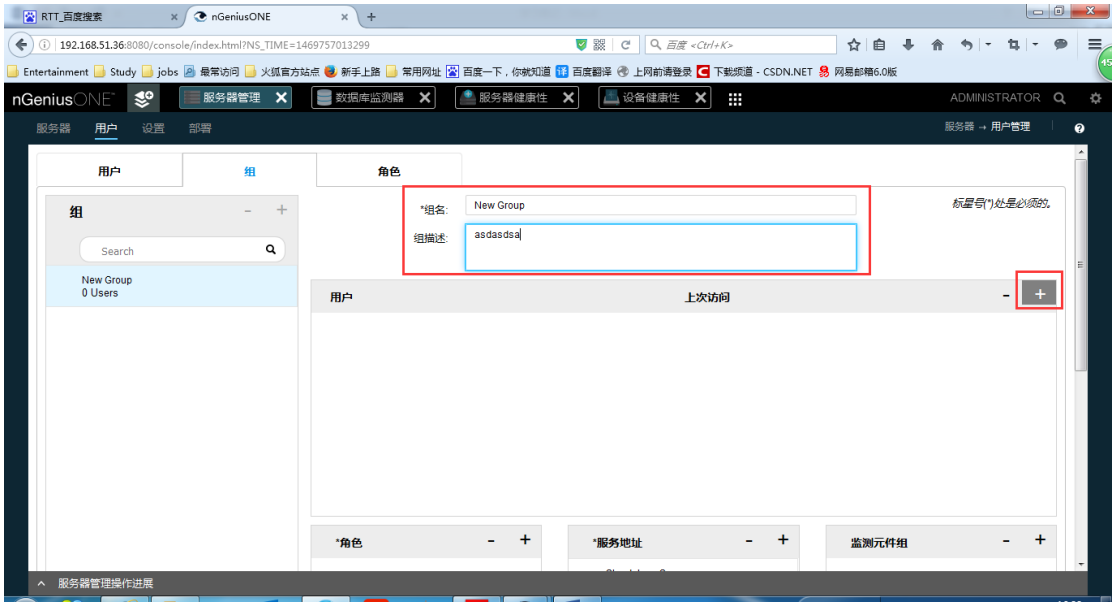
配置步骤（进行以下操作前必须具备 System Administrator 角色权限）

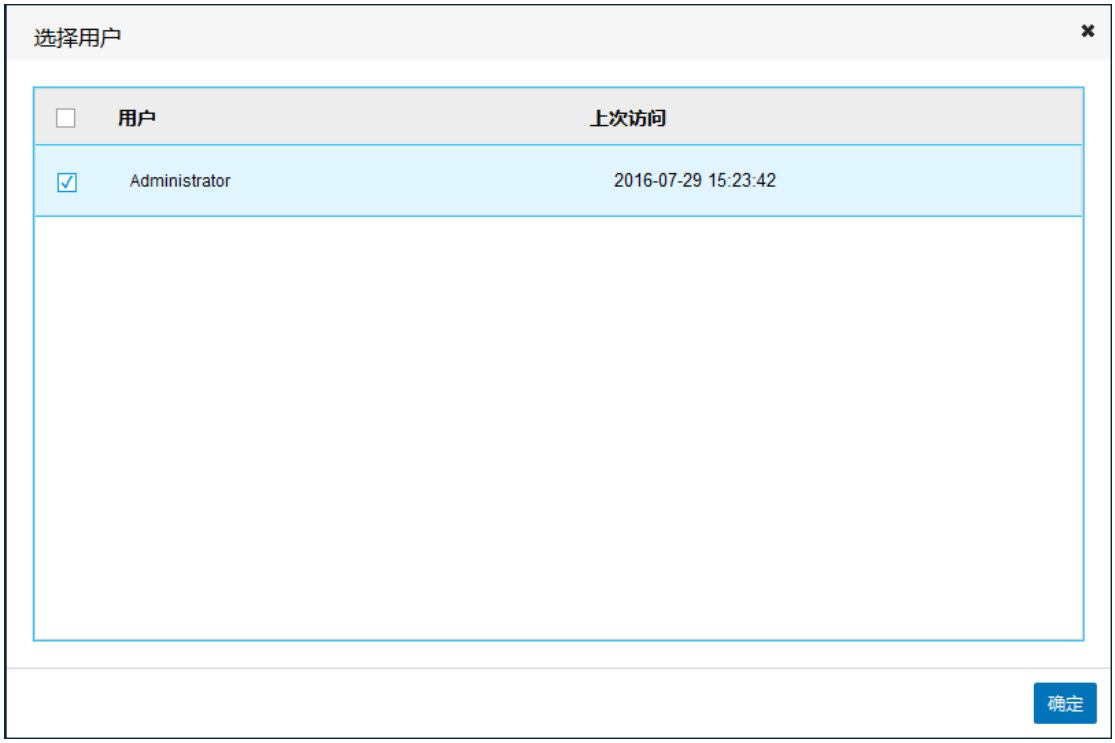
单击“配置管理器”→“服务器管理”图标，选择“用户”→“组”

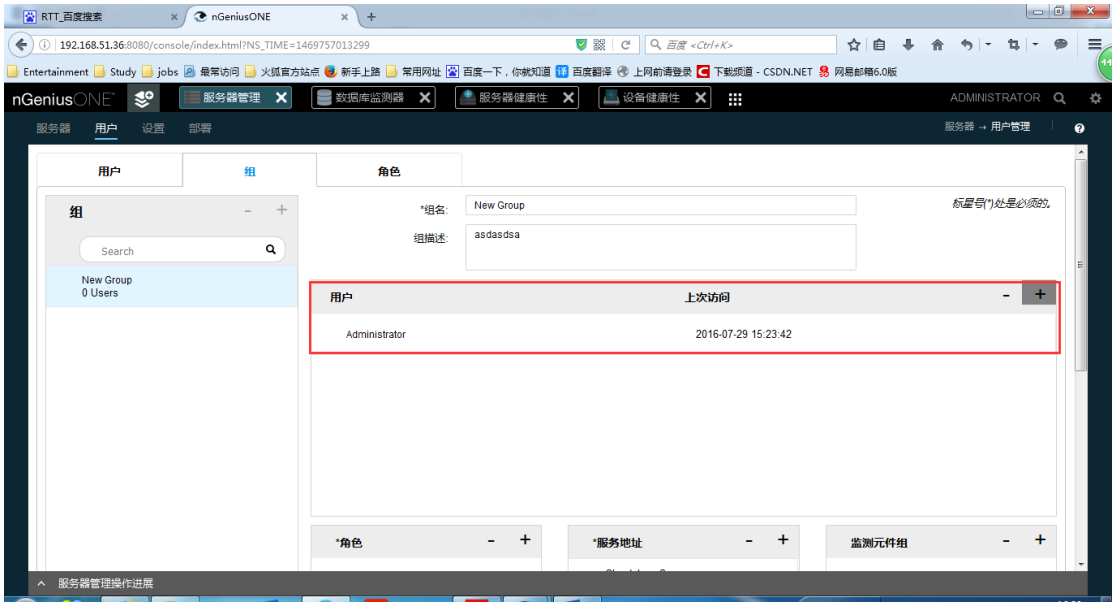
单击“添加”图标



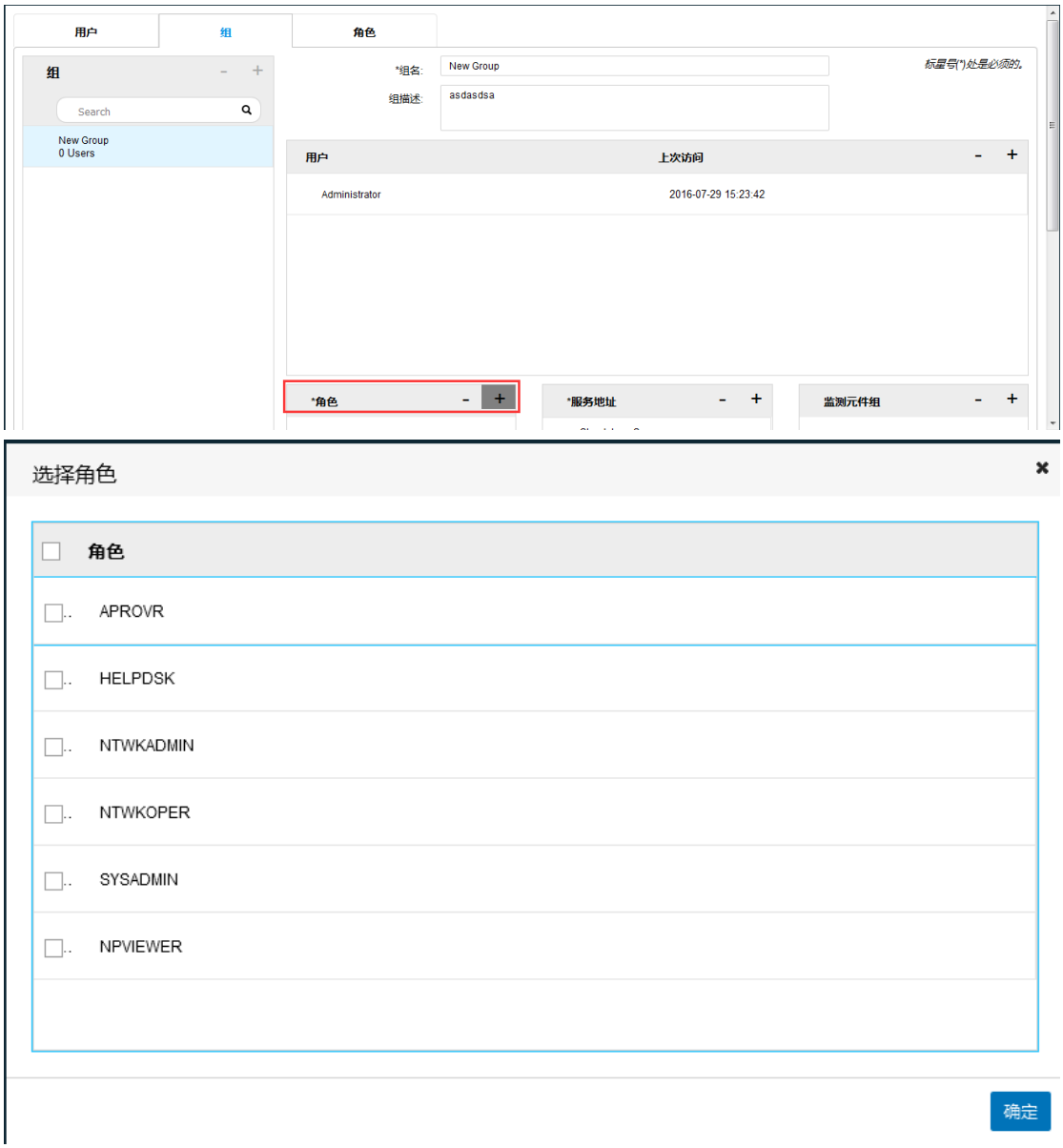
在界面输入一个组名（不支持空格和特殊字符）并进行简要描述，然后为该组添加成员，



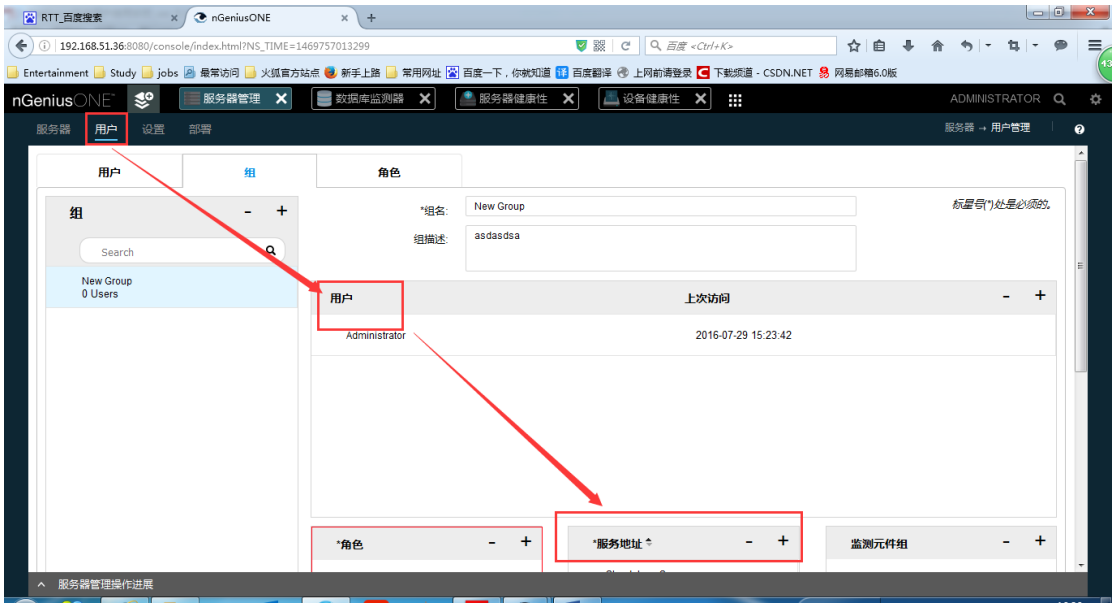


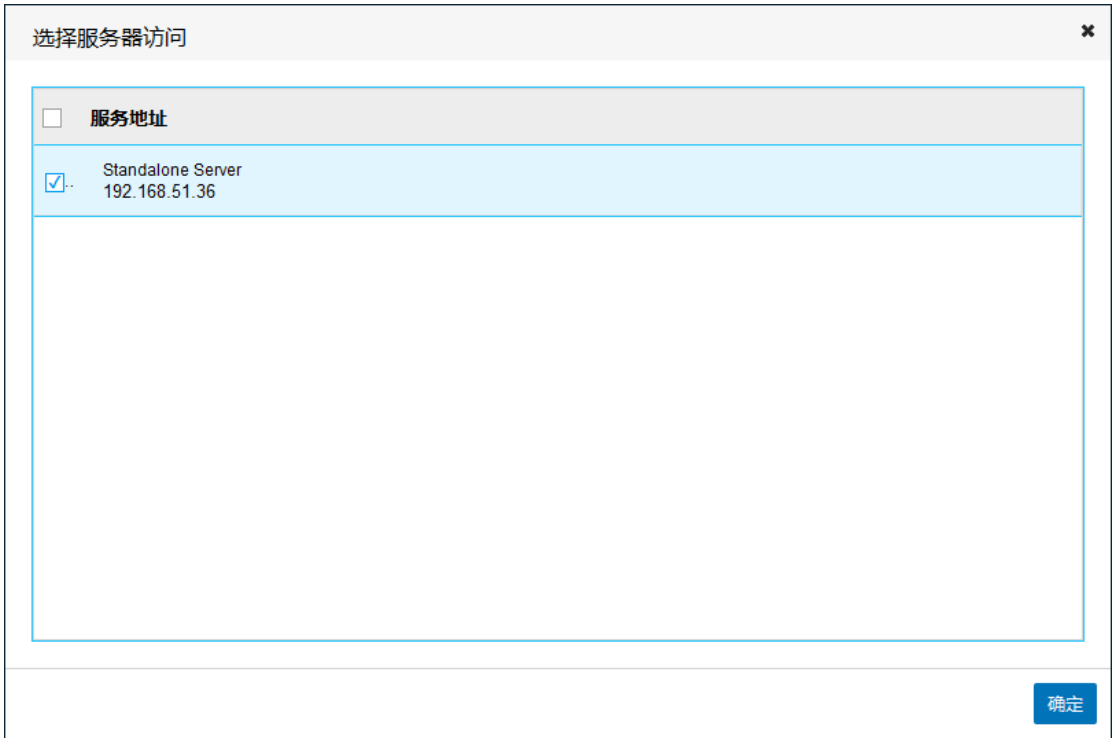


从“角色”下拉菜单中为该组分配一个或多个角色，如图



在“服务地址”部分，选择该组可以访问的 nGeniusONE 服务器成员，如图





在“解码选项”和“数据捕获”选项中设置相应的参数，如包头大小、数据包头等，如图

解码选项（Approver、Help Desk 和 Network Operator 角色所具备的）：

1） 选择“包头大小”并在 1-2048 范围内选择需要的大小来限制包头大小（默认是 64），

如果不填数值，当选择确认后将会设置成默认的 64bytes；

2） 选择“数据包头”选项来限制用户只能查看数据包头；

3） 输入数值 0 表示不限制包头大小；

Network Administrator（允许但不是必备的）：

1） 选择“包头大小”并在 1-2048 范围内选择需要的大小来限制分片大小（默认是 64）；

2） 选择“数据包头”选项来限制用户选择帧头；

注：如果适用，配置的分片大小将会传递给 Sniffer Analysis；但配置了第三方认证，认证所设置的分片大小会覆盖用户帐号所设置的尺寸；

数据捕获（组角色必须要分配 Network Administrator 角色）：

单击“覆盖”复选框允许组成员显示或清除从“Capture Status”视图中所捕获的所有数据；该选项默认是没有勾选的。

单击“确认”提交配置；

配置需要在组成员下一次登录时才生效；

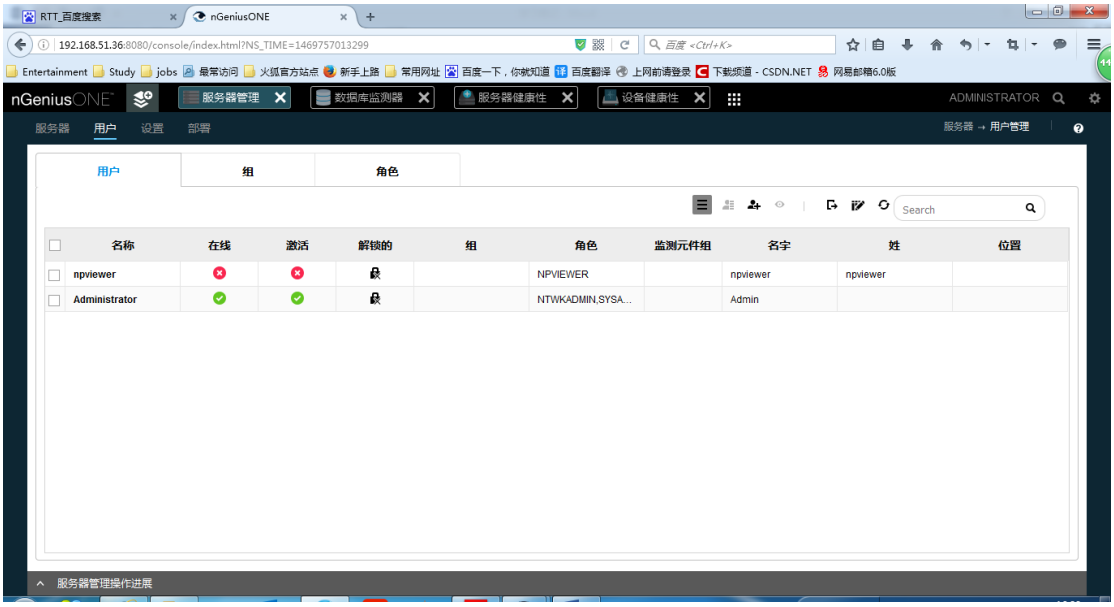
注：必须为每个组分配至少一个角色，如果分配角色过多，组成员将有权限使用更多的功能；

5.3 限制用户帐号权限

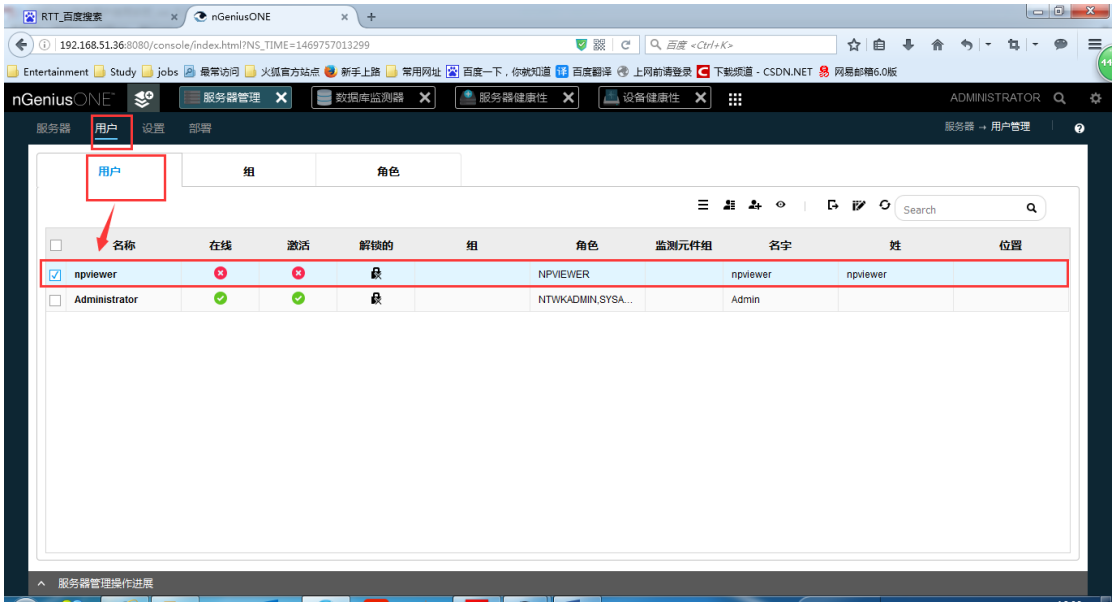
在创建用户帐号时，System Administrator 可以通过限制用户访问监控元件组来限制用户的权限。被限制的用户状态为覆盖原分配给该用户角色的已有权限。例如，作为 System Administrator 角色的用户被限制可访问的监控元件组后，从属于该帐号的用户变成了限制用户，作为限制用户，不再具备 System Administrator 角色的所有权限。

配置步骤：

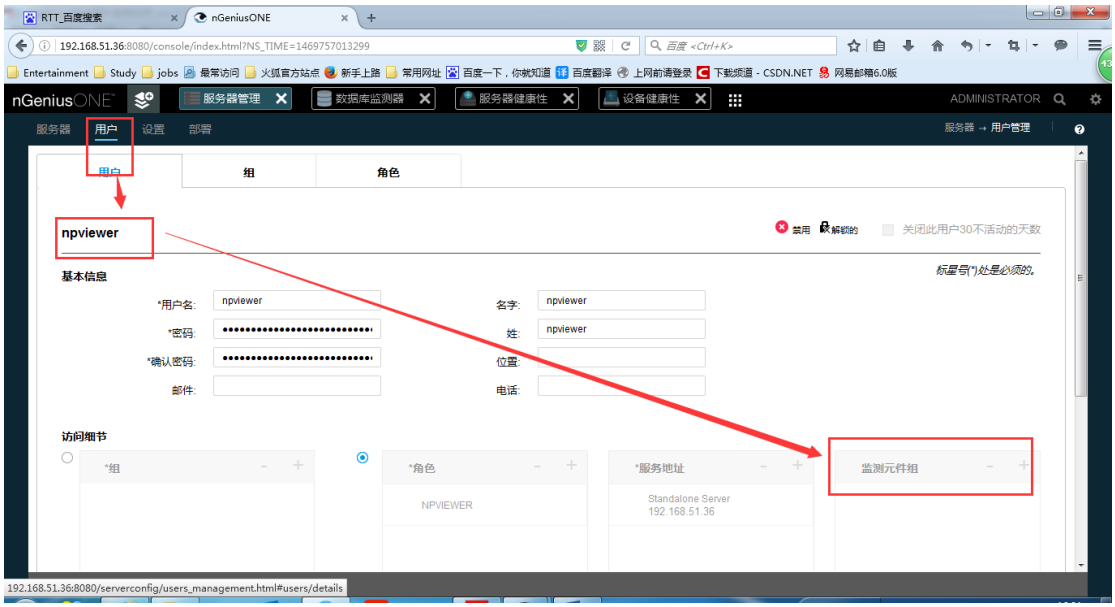
单击“配置管理器”→“服务器管理”图标，选择“用户”→“用户”，如图



选择复选框并单击一个已有用户，如图



查看“监控元件组”面板，列表中显示预先定义好的监控元件组，如图



单击一个或多个复选框为该用户进行关联相应的监控元件组并单击“确定”；

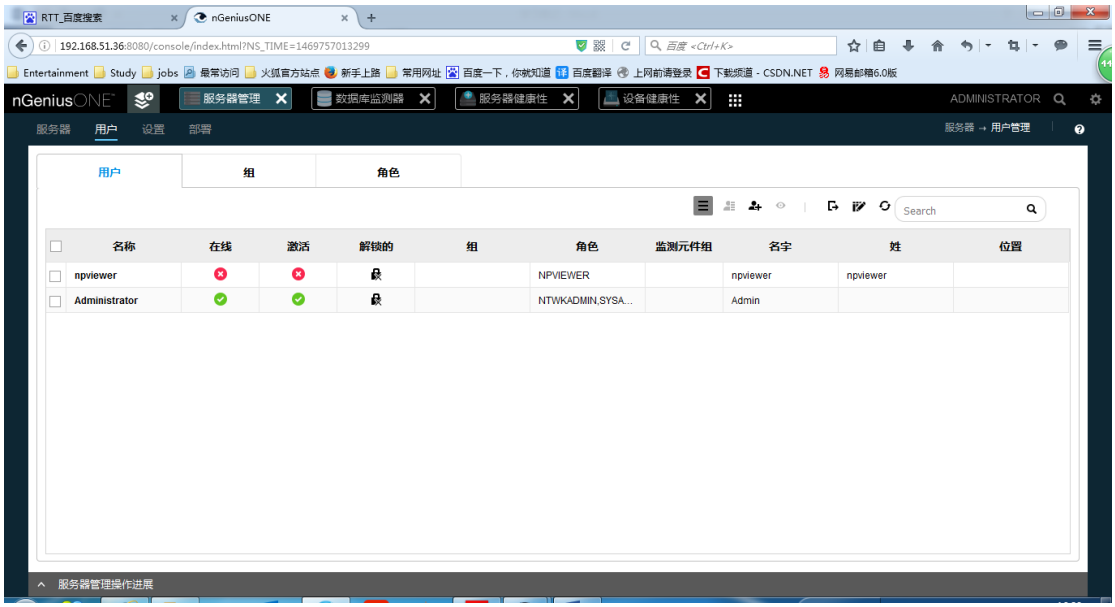
5.4 查看和管理用户帐号

日常监管和控制任何的 nGeniusONE 用户，系统管理员需要快速确定在 nGeniusONE 服务器上运行的所有在线会话的用户的 IP 地址和登录时间。根据需要可以中断任意会话除了管理会话以及当前登录会话。

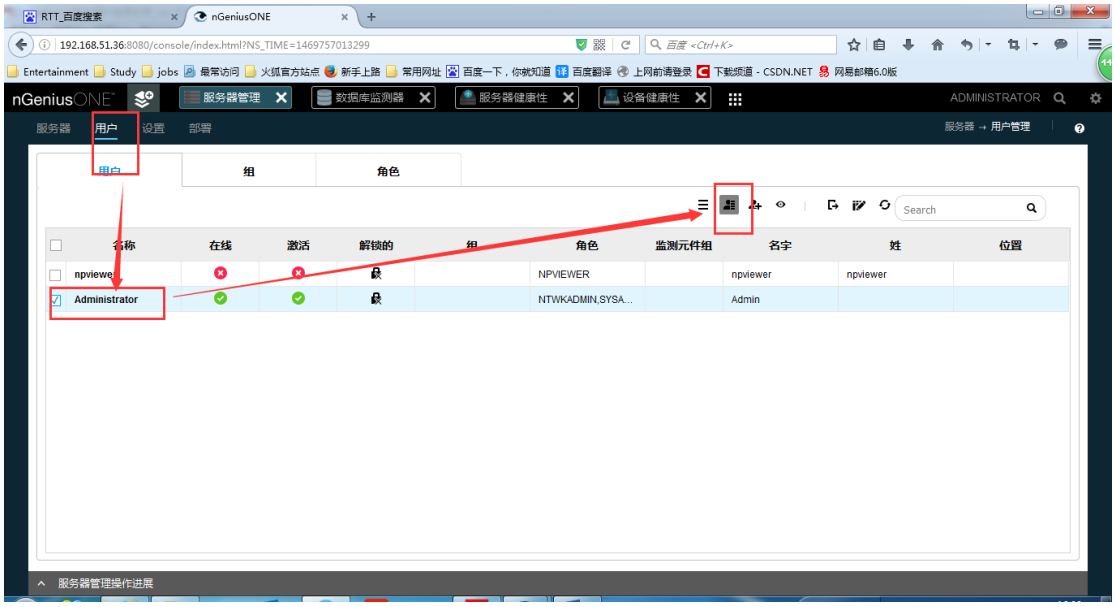
同时我们也可以禁用超过 30 天不在线的用户；另外，也可以通过手动给多次登录失败后被锁定的帐号解锁，系统默认在 30min 后也会自动解锁。

5.4.1 查看用户配置或会话，强制用户登出或中断用户会话

单击“配置管理器”→“服务器管理”图标，选择“用户”→“用户”，如图

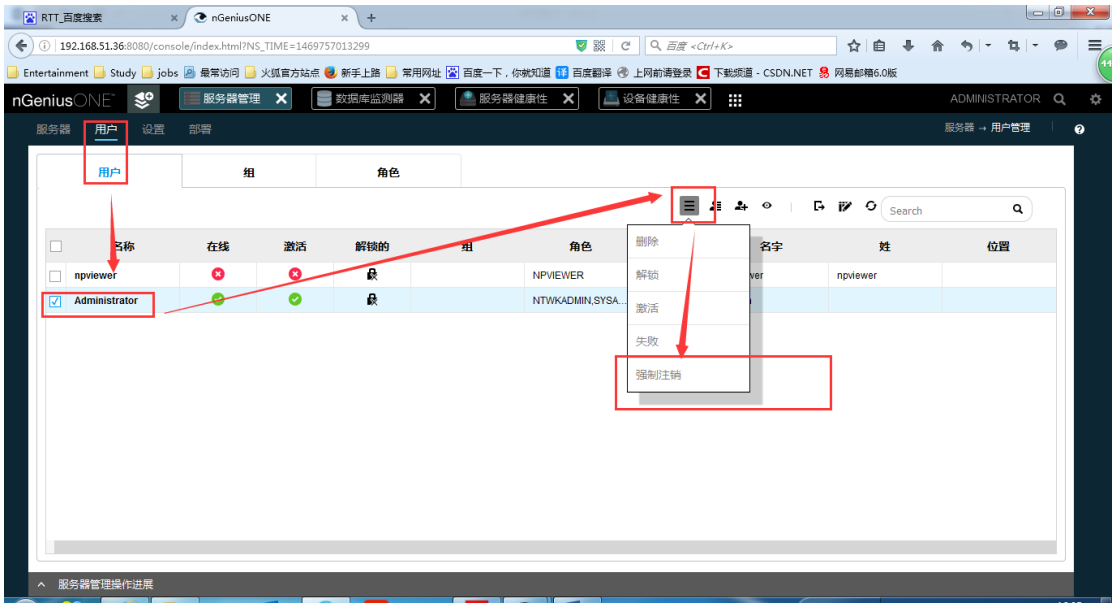


单击想要查看的用户的配置或会话的复选框，如图



单击“Sessions”查看特定用户当前所有登录会话，如图

如果需要强制用户登出，可以从“用户操作”图标下拉菜单中选择“强制注销”，一次只能关闭一个会话，如图

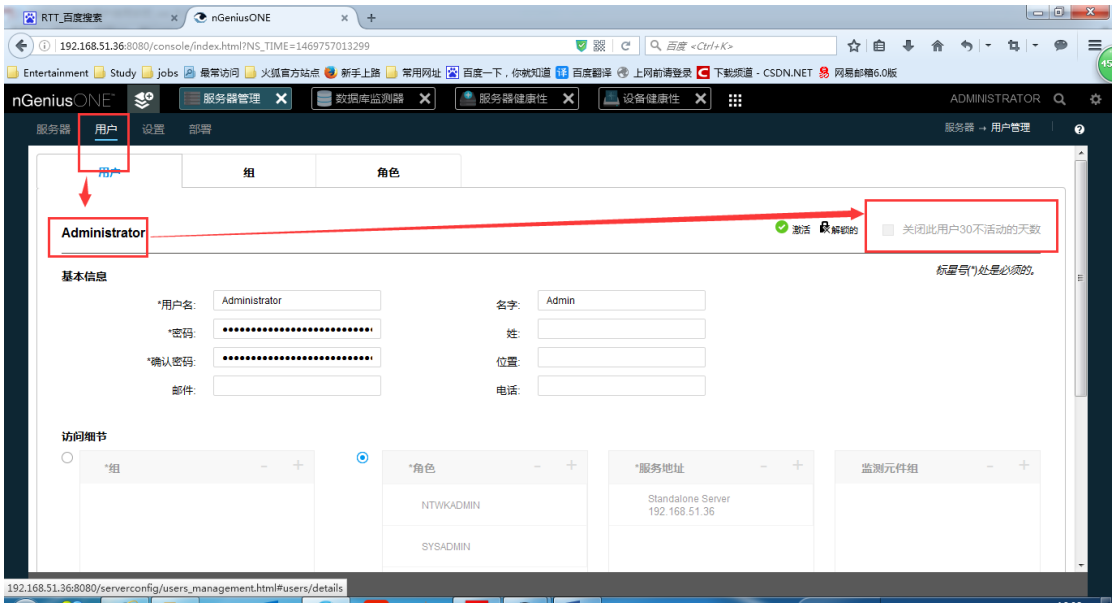


另外，如要关闭一个或多个用户会话（除了当前会话），单击对应的“会话”，然后选择“终止”，如图

最后单击“关闭”退出即可。

5.4.2 禁用用户

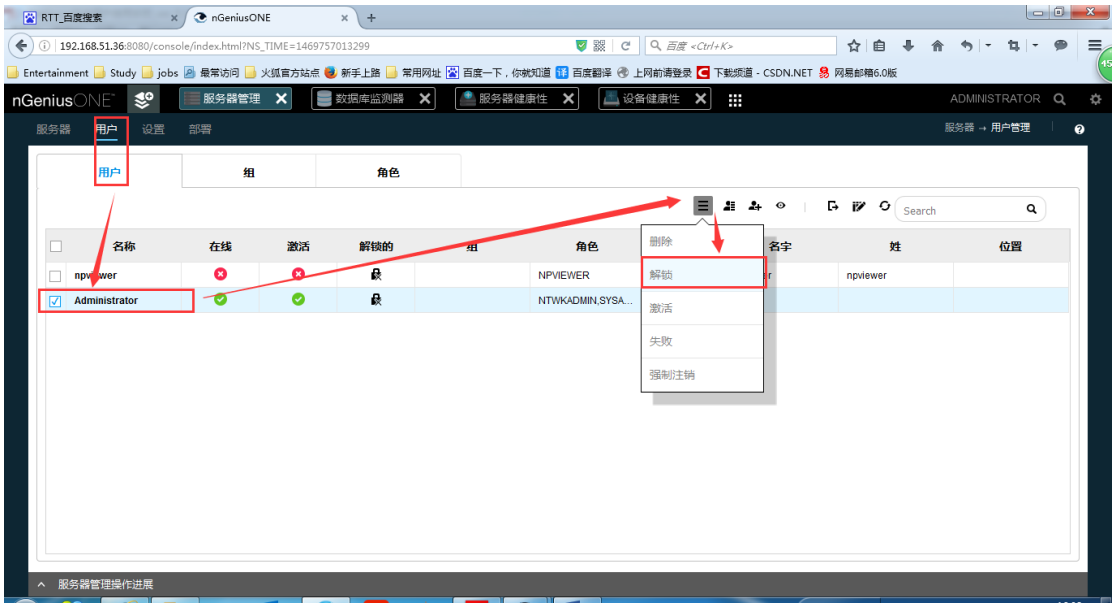
单击复选框“30 天都不在线的话禁用这个用户”并选择“确定”，如图（可以通过修改系统文件参数调整该时间参数）



5.4.3 解锁用户

选择对应的用户；

单击“解锁”然后选择“确定”，如图



5.5 配置 TACASE+认证服务

1. “所有模块”→“服务器管理”

2. “Settings”→“验证服务器”→“TACASE+”，进入配置界面

3. 填入以下参数：

① 服务器地址

② 服务端口（默认为 49）

③ 密钥，用于加密 nGeniusONE 服务器和 ACS 服务器之间的数据包。(在配置 ACS 认证服务器时，在 *key* 项(windows)或 *NAS Secret* 项填入该密钥)

④ 添加另一台认证服务器（可选项）

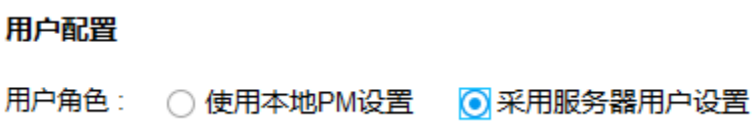
⑤ 本地端口，用于开始连接的本地端口，默认为 9540

⑥ 协议，与 NGENIUS 服务关联的协议，默认为 IP（对于 Windows ACS Server 必须为 IP）

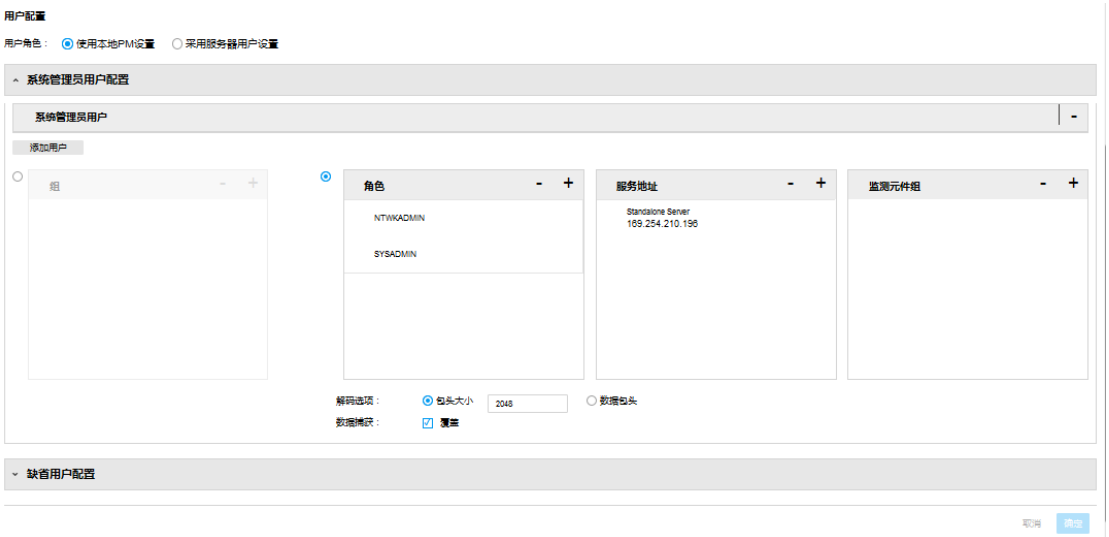
⑦ 服务，当选择”Ues server user settings”时自动填充为 NGENIUS

⑧ 超时时间，最大为 15 秒

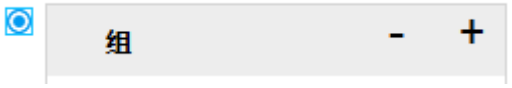
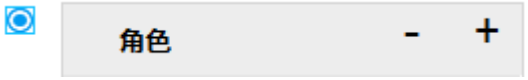
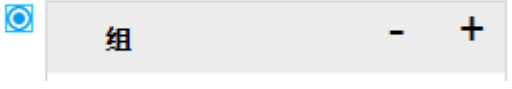
4. 选择用户角色

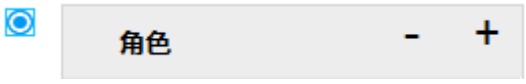


① 采用本地授权



系统管理员用户配置	
参数	描述
添加用户	点击 添加用户 打开系统管理员列表： ● 添加拥有管理权限的用户，以逗号分隔如：admin1,admin2 ● 删除不需要管理权限的用户 注意：NETSCOUT 强烈推荐至少分配一名系统管理员。在 nGeniusONE 系统中，只有系统管理员可以管理用户角色以及权限。如果 SYSADMIN

	列表中没有用户，那么用户管理功能就由默认拥有 HELPDSK 角色的用户定义，但该用户没有权限去管理用户和权限。
组	勾选  来添加或者删除用户组 来配置想要关联系统管理用户权限的用户组
角色/服务地址/监测元件组	勾选  来为系统管理用户添加或者删除角色/服务地址/监测元件组 ● 角色——想要关联到系统管理用户的角色。默认将 SYSADMIN 和 NTWKADMIN 分配给指定用户，让用户在外部认证启用后获得访问 nGeniusONE 所有功能模块的权限。 ● 服务地址——定义外部认证用户可以访问的 nGeniusONE 服务器。在分布式环境中，默认可访问所有本地服务器。也可以通过选择特定服务器地址来限制用户访问。 ● 监控元件组——定义外部认证用户可以查看的监控元件组
解码选项	● 包头大小——定义被授予 SYSADMIN 以及外部认证过的用户可捕获或解码的数据包大小，输入 0 代表无限制 ● 数据包头——限制用户只能查看数据包头。需要有 APPOVR,HELPDSK 以及 NTWKOPER 角色的系统管理用户
数据捕获	覆盖——允许 NTWKADMIN 去展示或者清空数据
缺省用户配置	
组	勾选  来添加或者删除用户组

	来配置想要关联系统管理用户权限的用户组
角色/服务地址/监测元件组	勾选  来为系统管理用户添加或者删除角色/服务地址/监测元件组 ● 角色——想要关联到系统管理用户的角色。默认将 SYSADMIN 和 NTWKADMIN 分配给指定用户，让用户在外部认证启用后获得访问 nGeniusONE 所有功能模块的权限。 ● 服务地址——定义外部认证用户可以访问的 nGeniusONE 服务器。在分布式环境中，默认可访问所有本地服务器。也可以通过选择特定服务器地址来限制用户访问。 ● 监控元件组——定义外部认证用户可以查看的监控元件组
解码选项	● 包头大小——定义被授予 SYSADMIN 以及外部认证过的用户可捕获或解码的数据包大小，输入 0 代表无限制 ● 数据包头——限制用户只能查看数据包头。需要有 APPOVR,HELPDSK 以及 NTWKOPER 角色的系统管理用户
数据捕获	覆盖——允许 NTWKADMIN 去展示或者清空数据

② 采用 ACS 服务器授权

在下表中提供 TACACS 服务器中的客户属性名称，每个框都必须填写并且必须和 ACS 服务器中的设置匹配。通常，NETSCOUT 推荐使用默认配置。详细配置步骤见本小节末尾附件。

当时使用 ACS 服务器设置做认证时，所有新的或已有的用户账号信息必须通过 Cisco

Secrue ACS 系统来维持。系统管理员在 nGeniusONE 中唯一可以做的用户操作就是在用户界面中配置用户权限。

5. 点击“确定”应用配置。

6. 点击界面左方的 来将认证方式改为 TACACS+

7. 重启 nGeniusONE 服务

附：

一、思科 ACS 配置方法(PDF)

Integrating_PM_Cisco_ACS_5x_733-

二、添加授权参数认证

当使用 ACS 做授权时，ACS 服务器的管理员需要添加“NSROLES”、“NSPROFILE”、

“NSSERVERLIST”参数

NSROLES：定义通过 ACS 认证的用户所使用的 nGeniusONE 服务器角色

语法：NSROLES=<user role1>[,<user role2>,<uers role3>，...]，输入一个或多个 nGeniusONE 服务器预定义的角色，以逗号分隔。

nGeniusONE 服务器预定义角色：

- NTWKOPER——Network Operator
- SYSADMIN——System Administrator
- NTWLADMIN——Network Administrator
- APROVR——Approver
- HELPDSK——Help Desk

例如，为一个用户分配角色 Network Administrator 和 System Administrator，输入如下：

NSROLES=NTWKADMIN,SYSADMIN

NSPROFILE：定义用户参数，所有项均为必填

语法：

NSPROFILE=<Firstname>,<Lastname>,<emailaddress>,<data_capture_slice_size>,

<override_data_capture>,<restrict_frame_header>

Firstname、Lastname、emailaddress 三项必须填入，邮箱格式必须为 name@domain。

data_capture_slice_size 为个人可以捕获以及解码的数据包字节数，范围 1-2048，输入 0 代

表无限制；

override_data_capture 参数允许分配了 Network Administrator 角色的用户查看或删除其他

用户捕获的数据。输入 1 开启该功能，输入 0 关闭；（注：如果用户未被分配 Network Administrator 角色，nGeniusONE 服务器忽略该参数）；

restrict_frame_header 参数限制用户只到帧头，输入 1 开启该功能，输入 0 关闭。

例如，限制用户 John Doe 切包大小为 1512 字节，override_data_capture 关闭，restrict_frame_header 开启，输入如下

NSPROFILE=John,Doe,jdoe@mycompany.com,1512,0,1

NSSERVERLIST：定义用户可登陆的 nGeniusONE 服务器

语法：NSSERVERLIST=ALL|<ipaddress1[,ipaddress2,ipaddress3,...]>

输入输入一个或多个 nGeniusONE 服务器地址，以逗号分隔；或者输入 ALL 来允许用户登录所有可用服务器。

例如：NSSERVERLIST=ALL/NSSERVERLIST=192.168.143.1,192.168.143.2

三、添加组认证：

ACS 服务器管理员可以为同一个组内的所有成员分配相同的参数，通过在组配置中添加“NSROLES”、“NSPROFILE”、“NSSERVERLIST”参数来完成。

小组内成员也可以单独做配置，个人配置总是优先于组配置。

NSROLES: 定义组内用户所使用的 nGeniusONE 服务器角色

语法：NSROLES=<user role1>[,<user role2>,<uers role3>, ...]，输入一个或多个

nGeniusONE 服

务器预定义的角色，以逗号分隔

nGeniusONE 服务器预定义角色：

- NTWKOPER——Network Operator
- SYSADMIN——System Administrator
- NTWLADMIN——Network Administrator
- APROVR——Approver
- HELPDSK——Help Desk

例如，为一个组分配角色 Network Administrator 和 System Administrator，输入如下：

NSROLES=NTWKADMIN,SYSADMIN

NSPROFILE：定义组参数，所有项均为必填

语法：

NSPROFILE=<Firstname>,<Lastname>,<emailaddress>,<data_capture_slice_size>,

<override_data_capture>,<restrict_frame_header>

当为一个组定义 NSPROFILE 时，Firstname、Lastname、emailaddress 三项也必须填入，Firstname、Lastname，但邮箱格式必须为 name@domain。

data_capture_slice_size 定义了组可以捕获以及解码的数据包字节数，范围 1-2048，输入

0 代表无限制；

override_data_capture 参数允许分配了 Network Administrator 角色的组查看或删除其他

用户捕获的数据。输入 1 开启该功能，输入 0 关闭；（注：如果组未被分配 Network Administrator 角色，nGeniusONE 服务器忽略该参数）；

restrict_frame_header 参数限制组只到帧头，输入 1 开启该功能，输入 0 关闭。

例如，限制一个组切包大小为 64 字节，override_data_capture 关闭，restrict_frame_header 开启，输入如下

NSPROFILE=network,admin,netwadmin@mycompany.com,64,0,1

NSSERVERLIST：定义组可登陆的 nGeniusONE 服务器

语法：NSSERVERLIST=ALL|<ipaddress1[,ipaddress2,ipaddress3,...]>

输入输入一个或多个 nGeniusONE 服务器地址，以逗号分隔；或者输入 ALL 来允许组登录所有可用服务器。

例如：NSSERVERLIST=ALL/NSSERVERLIST=192.168.143.1,192.168.143.2

6. 使用场景 – How to

How-To and Answer

一、如何通过服务仪表盘和服务监测器分析故障

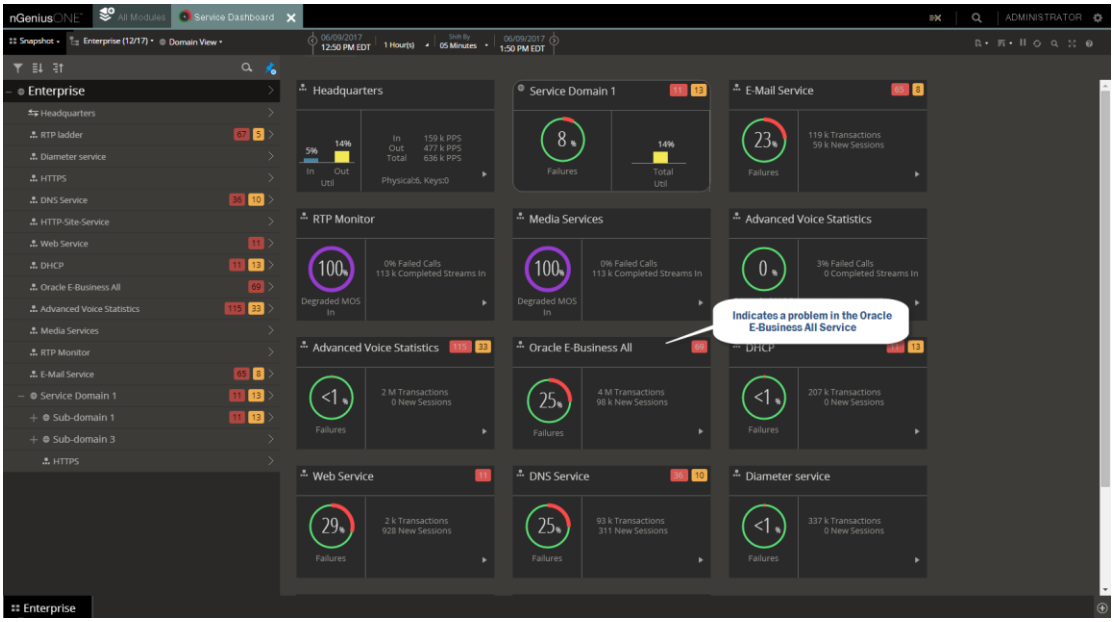
通过服务仪表盘和服务监测器分析问题主要遵循以下三个步骤：

- 定位故障应用
- 应用问题定位
- 会话分析

下面，我们以 Oracle E-Business 应用为例展示故障分析流程。运维人员收到用户电话，称访问数据库时出现问题，我们通过上述三个步骤对该故障进行分析。

1. 定位故障应用

从服务仪表上发现，应用服务“Oracle E-Business ALL”在过去一个小时的交易失败率为 25%

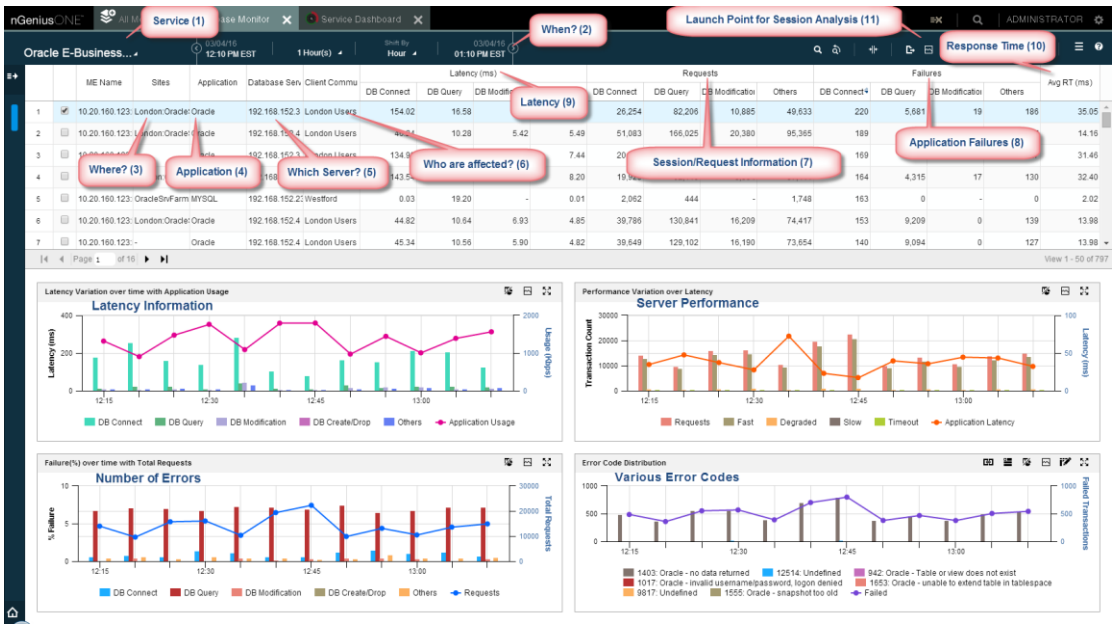


2. 应用问题定位

点击“Oracle E-Business ALL”的表盘，下钻至对应的服务监测器。在服务监测器中包含了以下内容：

1) 受到故障影响的服务
2) 故障发生时间段
3) 发生故障的 site
4) 引起故障的应用
5) 出现故障的服务器
6) 受到故障影响的客户端
7) 请求信息
8) 应用错误
9) 延时
10) 响应时间
11) 会话分析启动按钮

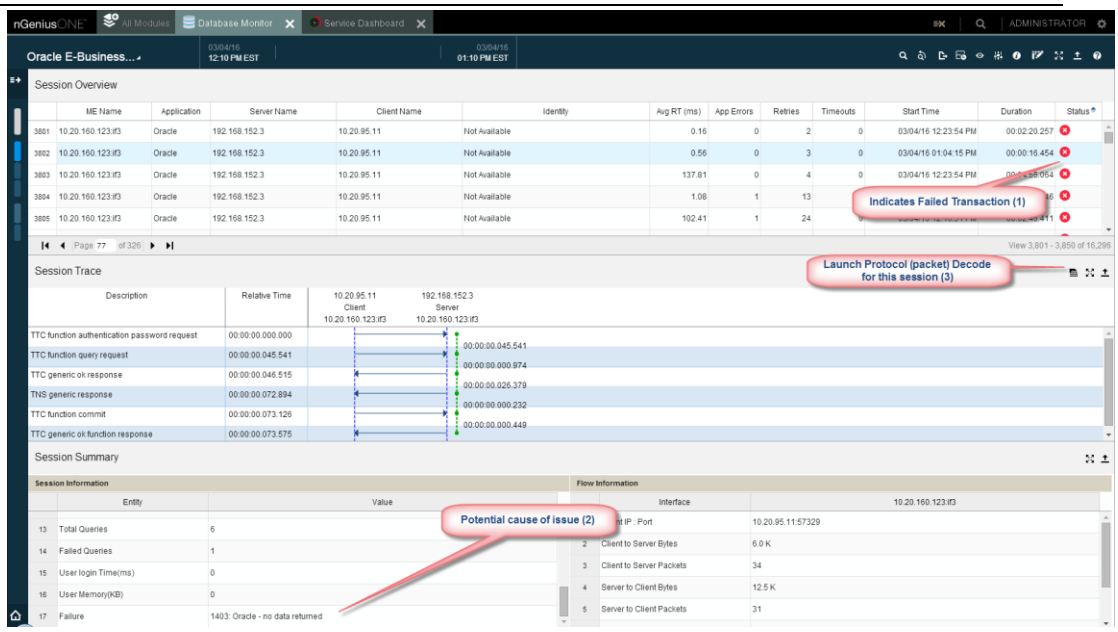
查看右下方的应用错误代码分布，能看到出现大量同一类型的应用错误。要查看更详细的信息，点击监测器界面右上方的会话分析按钮，启动会话分析功能。



3. 会话分析

会话分析界面展示了通讯过程中的每一个会话，在该界面有如下内容：

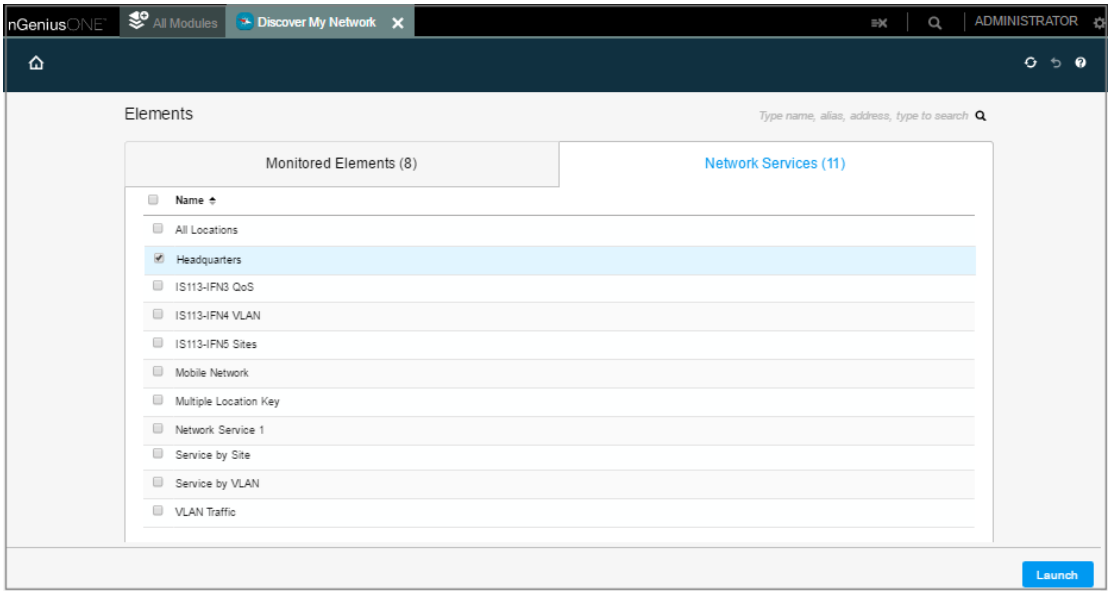
1) 会话状态（ 表示会话成功， 表示会话失败）
2) 会话信息（包括通讯对地址、通讯端口、错误代码等信息）
3) 数据包解码启动按钮


Indicates Failed Transaction (1)
Launch Protocol (packet) Decode for this session (3)
Potential cause of issue (2)

二、如何快速查看流量中的应用成分

除了服务、网络和流量监测器之外，“发现我的网络”模块也能提供网络活动的全局视图，用于临时排障。用户可以通过模块中提供的带有可视化图表的交易数、吞吐量、TCP 窗口情况以及数据包量等指标去分析网络负载以及应用失败。该模块同样可以通过高级视图展示媒体流量。

点击  图标进入“发现我的网络”模块后，勾选一个或多个探针接口并点击“运行”来进入监测器界面。



在“发现我的网络”界面中展示了过去一小时内选中探针接口下的各个应用，在上方的表格中包含了如下信息：

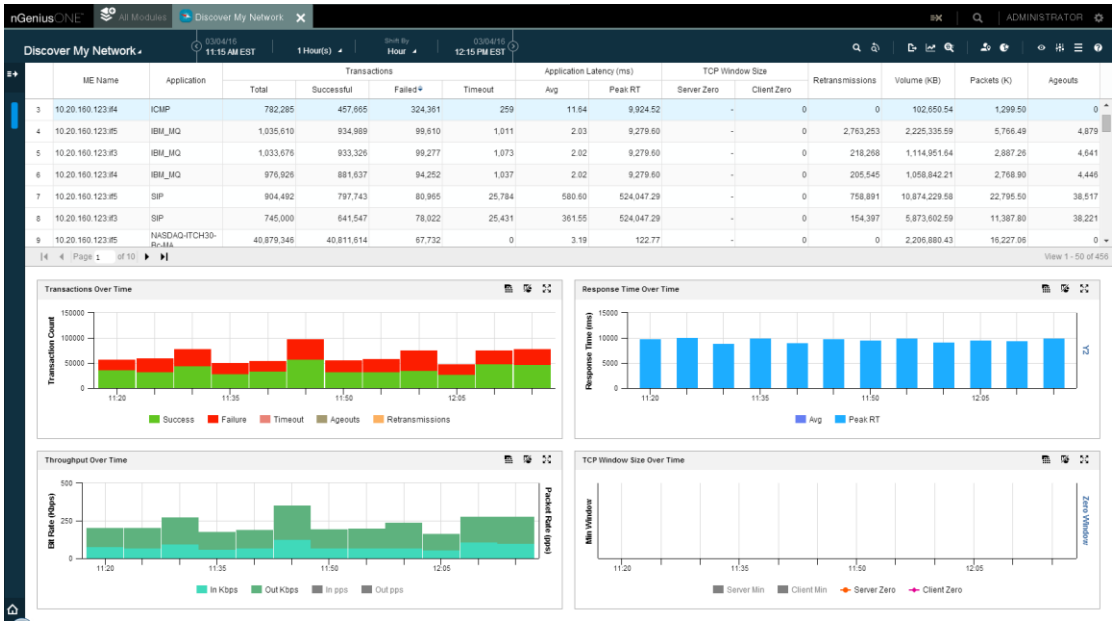
- 应用名称
- 交易信息
- 应用延迟情况
- TCP 窗口大小
- 流量总量（KB）
- 数据包总量（K）
- 超时

下方四个图表展示了应用的如下信息：

- 交易量

- 响应时间
- 应用吞吐量（比特率）
- TCP 窗口大小

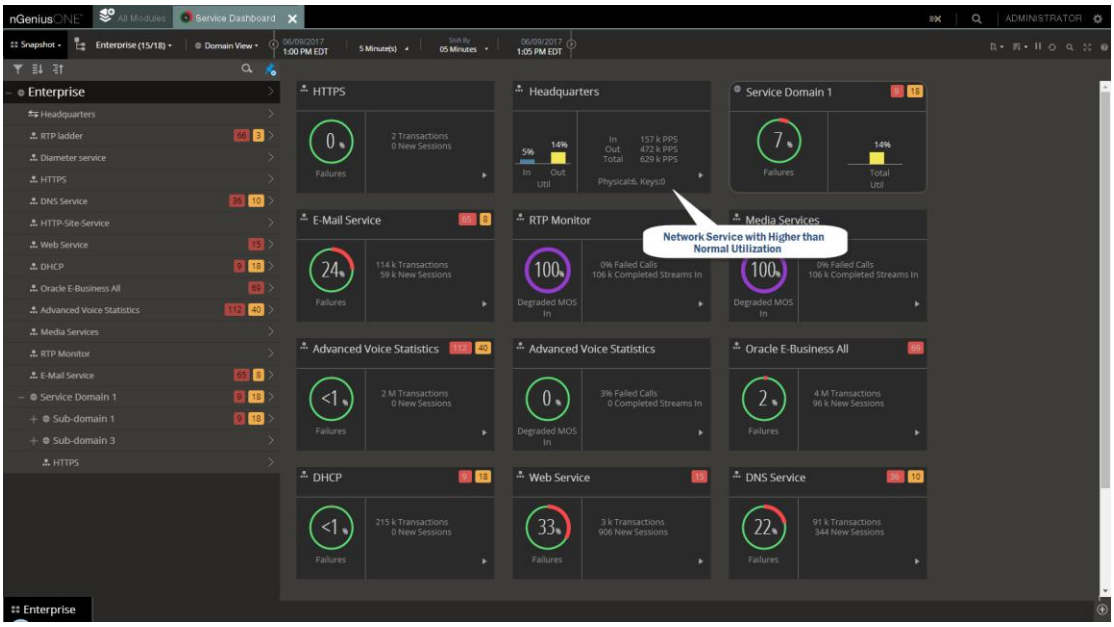
用户可以选中特定应用并点击  图标跳转至应用对应的服务监测器做更深入的分析。



三、如何通过服务仪表盘和应用监测器分析利用率增长

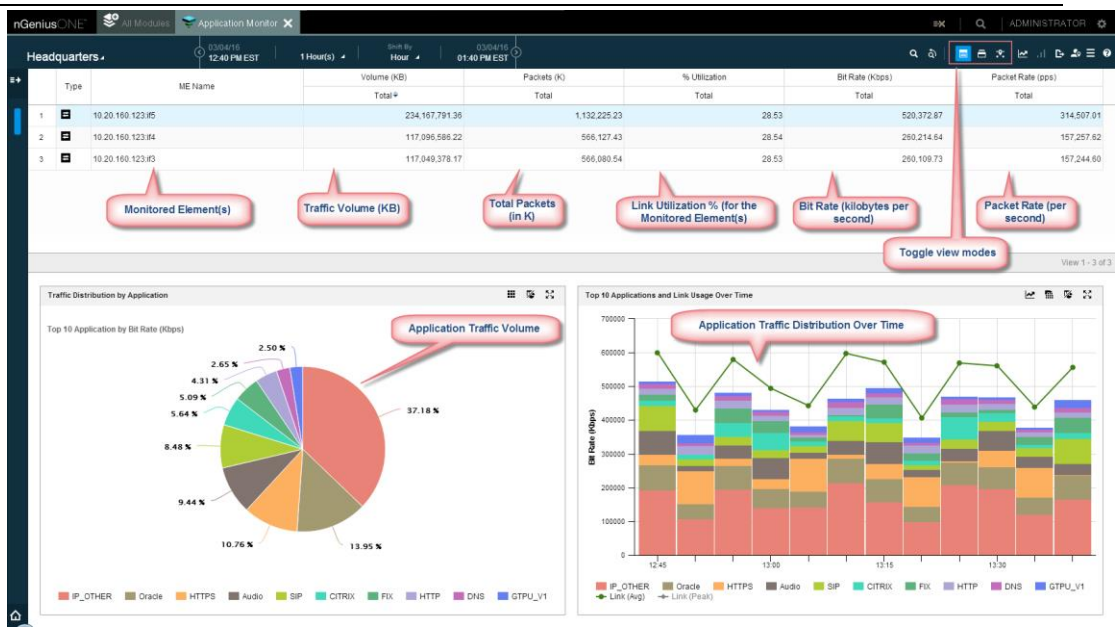
nGeniusONE 服务仪表盘可以展示 ASI 物理接口以及网络服务的吞吐量。通过服务仪表盘，用户可以监控指定网络中的特定问题以及查看特定网段的带宽。

如下图，网络服务“Headquarters”的利用率高于平时的正常范围，“out”方向将近 14%，“in”方向为 5%。为了查看更详细的信息，点击表盘下钻至监测器中



点击网络服务对应的表盘会跳转至应用监测器，该监测器上方表格展示了总字节数、总数据包量以及网络服务的利用率，下方图表展示了带宽占比前十的应用及其流量时间分布曲线。

如下图，可以从左下方的饼状图中看到未定义的应用流量占 37%，Oracle 流量占 13.95%。用户还可以在右下方的柱状图查看过去一小时中应用流量按时间分布的曲线。

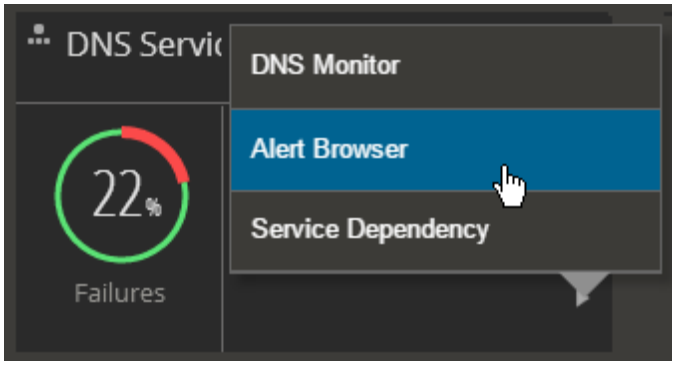


通过应用监测器可以发现，导致网络服务 Headquarters 在 out 方向利用率增长的是未定义应用的流量，用户便可以针对该流量进行处理。

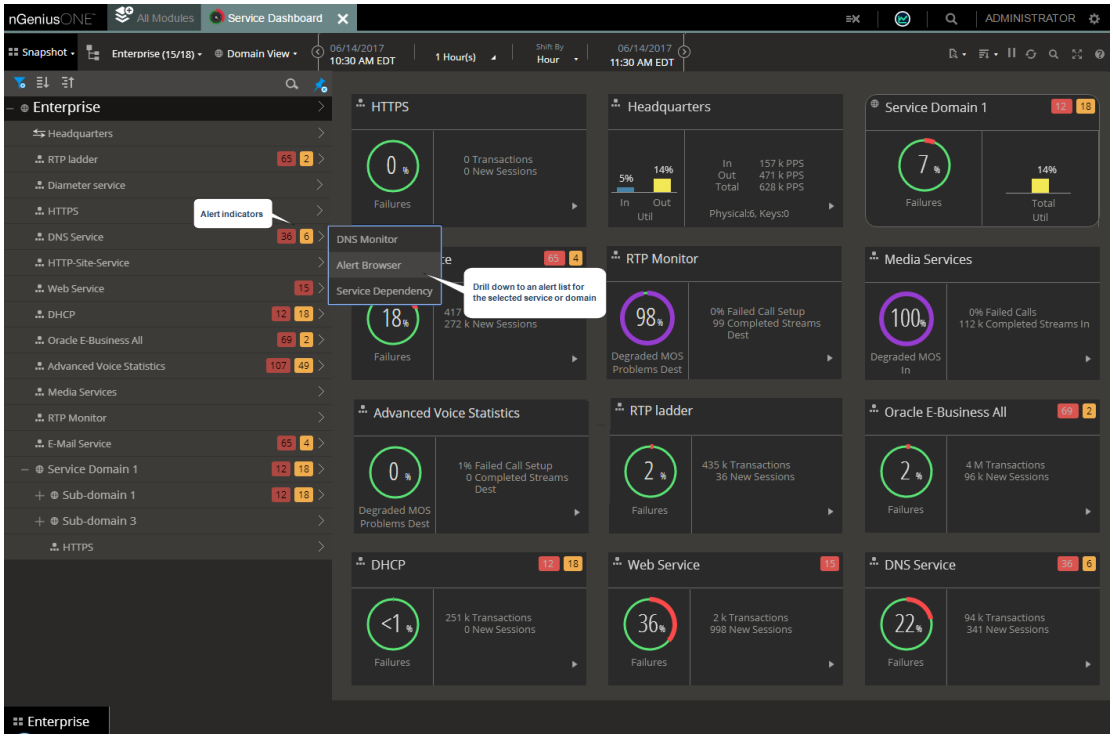
四、如何查看服务告警

当为服务配置的告警触发器被触发时，会生成服务告警。有以下几个途径去查看告警：

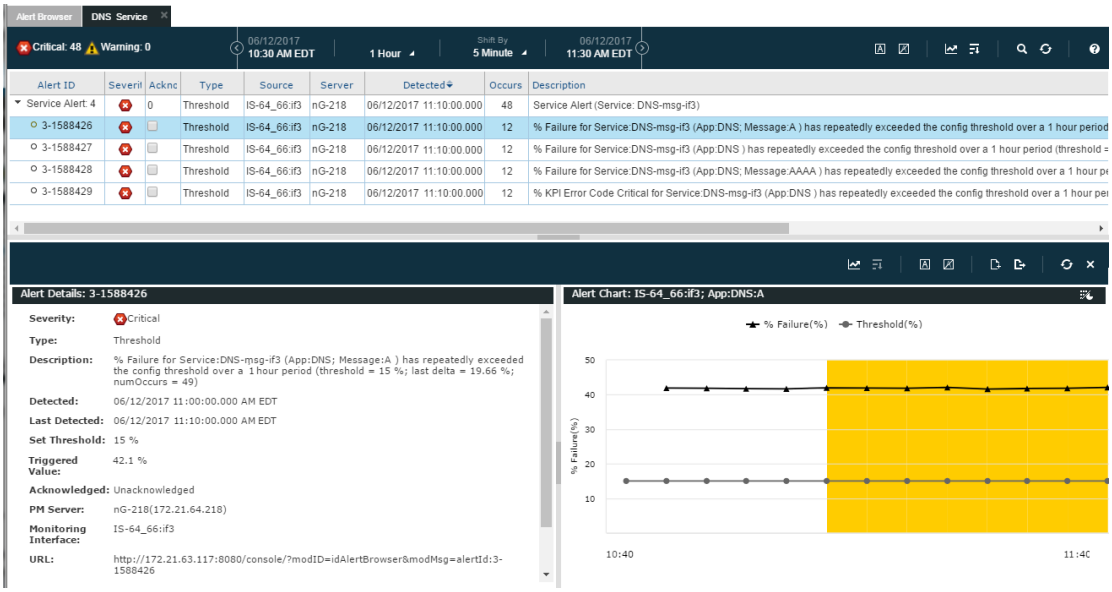
- 在 nGeniusONE 服务仪表盘上，点击某个服务的表盘，并选择“告警浏览器”



- 在服务层级树中选中服务，并点击“告警浏览器”



如下图，用户发现 DNS 服务出现告警，并通过上述两种方式进入告警浏览器查看告警详情。在告警浏览器中，选定时间段内与该服务相关的告警会全部陈列出来，点击其中一条告警可查看告警详情。



在多数情况下，告警浏览器中的告警详细信息能够支持用户完成排障。但如果用户需要更多的信息来进行故障分析，可以通过  按钮下钻至服务对应的服务监测器中查看。

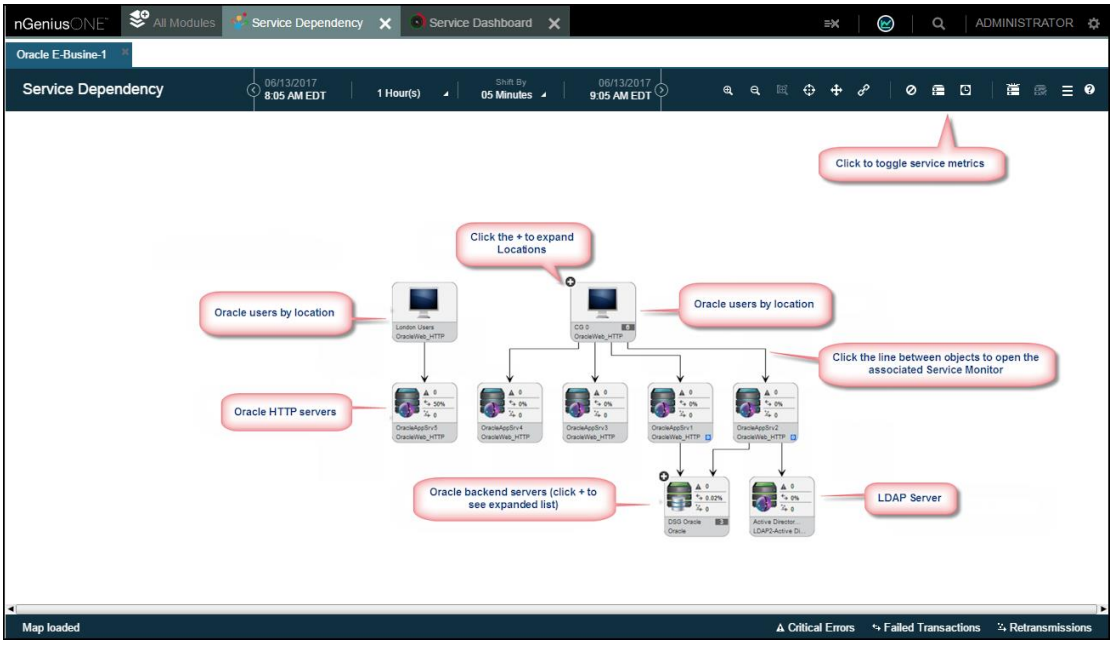
五、如何排查出现在业务访问路径上的故障

“服务依赖性”工具重点关注关键应用的服务器间和服务器与客户端间的通讯，用户可以通过该工具：

- 了解应用服务器间的访问路径；
- 了解整个业务的结构、使用情况以及潜在的瓶颈点；
- 找出引起故障或不应该出现在访问路径中的服务器节点；

用户可通过服务仪表盘左侧的“服务层级树”→“服务依赖性”打开该工具

服务依赖性提供了应用服务内各个应用服务器、对应客户端以及提供辅助功能（如 DNS、LDAP、RADIUS）的服务器间的访问关系。用户可以通过右键点击节点之间的连接线下钻至关联的服务监测器。



下图展示了服务依赖性界面中可展示的指标（失败、服务器负载、延迟）

失败：


0
8.33%
0
192.168.60.35
Oracle
Critical Errors
Failed Transactions
Retransmissions

服务器负载：

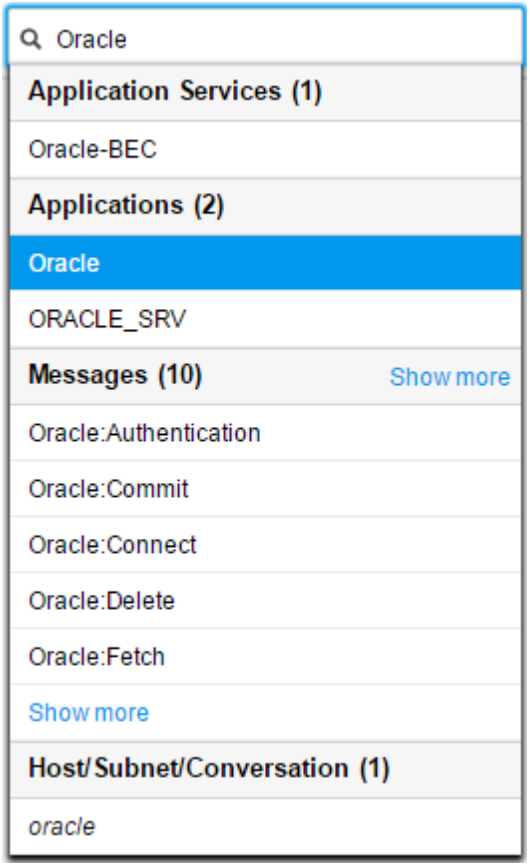

12
0
1
192.168.60.35
Oracle
Total Requests
Transaction Rate
New Sessions

延迟：

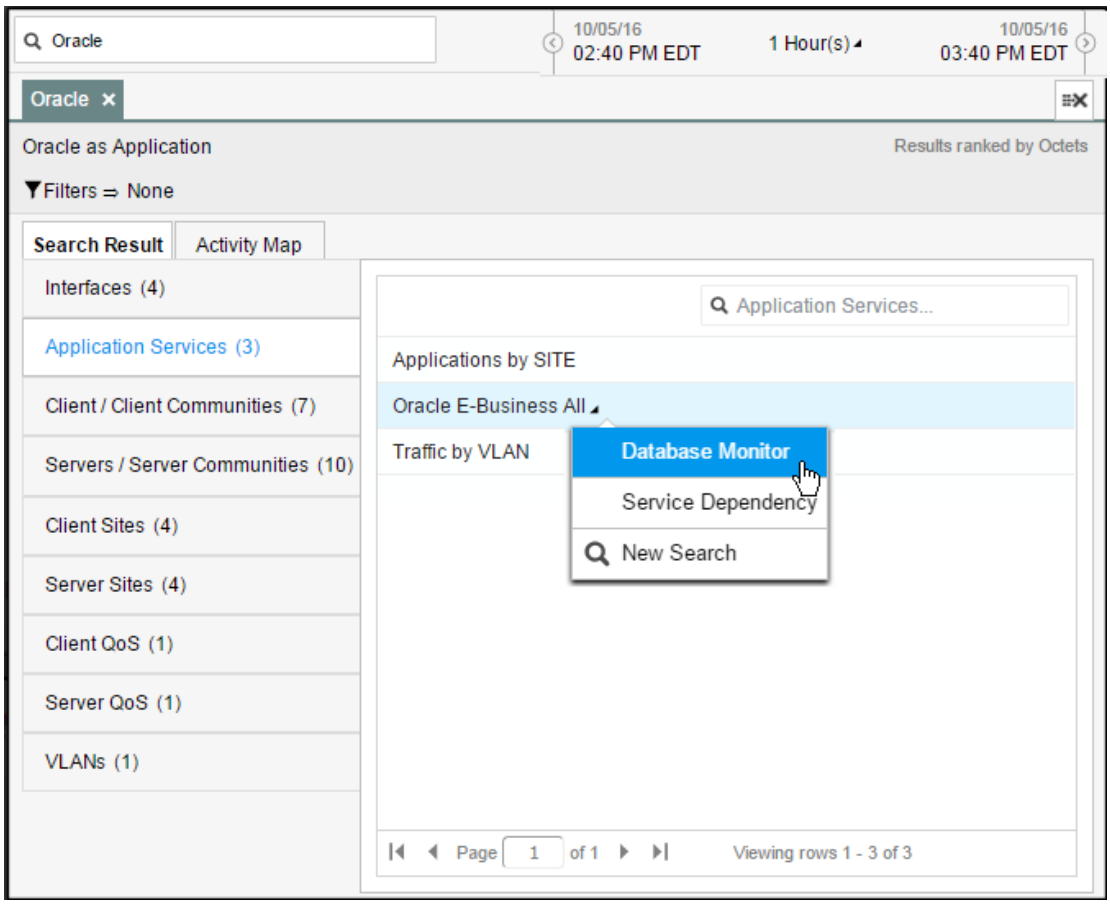

0 ms
0%
0
192.168.60.35
Oracle
Average Response Time
Slow Responses
Timeouts

六、如何快速查找想要查看的信息（如应用、主机或通讯对等）

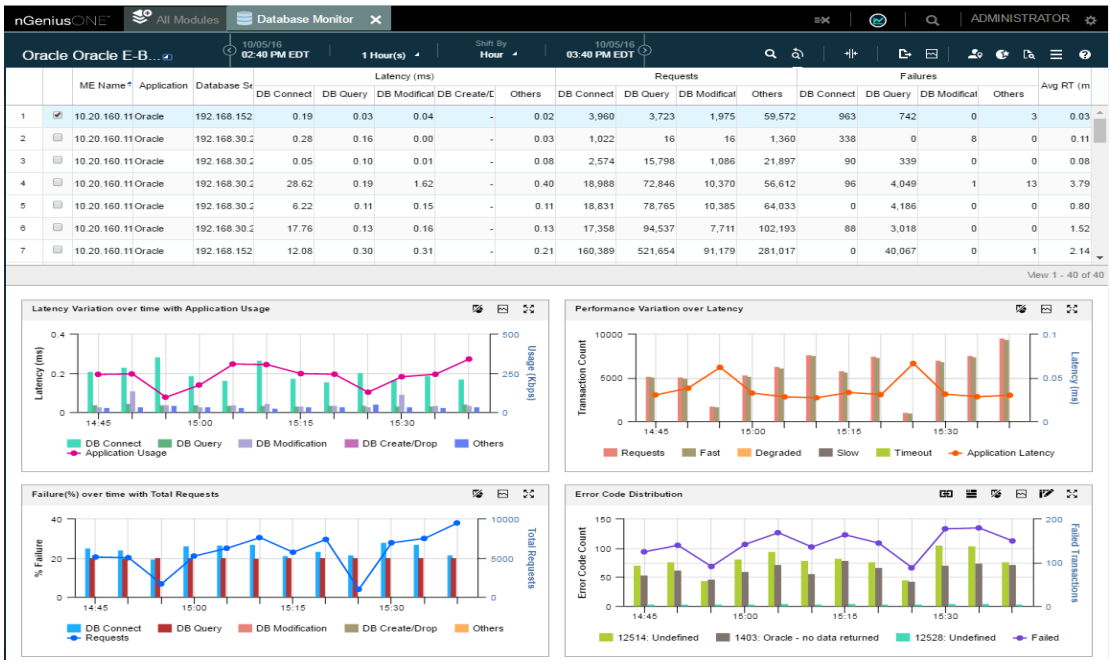
用户可以在“全局搜索”功能中查找感兴趣的应用、主机或通讯对。如下图，用户想查找 Oracle 相关的条目，点击 nGeniusONE 界面右上方的“全局搜索”按钮，在搜索框内输入 Oracle，nGeniusONE 会列出所有匹配的条目，选择 Oracle 应用。



在搜索结果中查看感兴趣的部分（如应用服务）



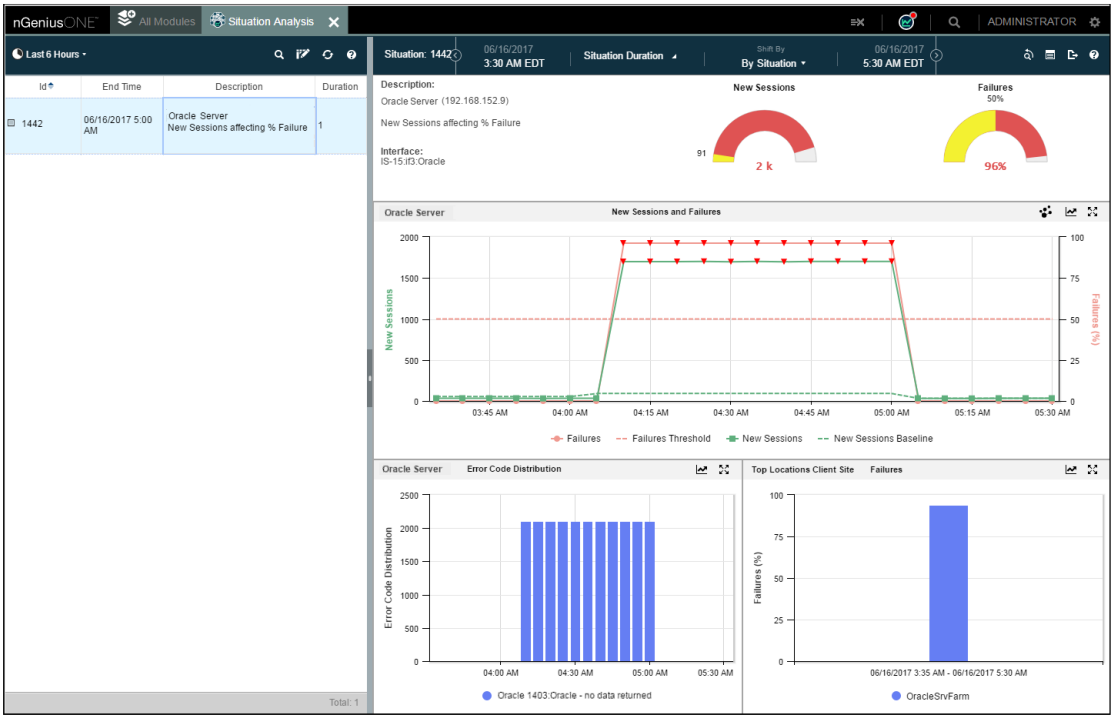
想查看应用服务“Oracle E-Business ALL”更详细的信息，可点击对应应用服务的 图标，打开应用服务关联的服务监测器，如下图为数据库监测器。



七、如何通过场景分析模块找到数据库交易失败的原因

用户可以通过“场景分析”模块在客户投诉前先一步找到数据库出现的问题。当新问题出现时，场景分析模块会以红点标识。

点击红点打开场景分析模块，新出现问题陈列在界面左侧，右侧则是对问题的详细描述。在描述中能够看到交易失败发生的位置、原因以及相关的错误代码。



问题描述的内容包括：

1) 概述

- 出现问题的 Oracle 应用及服务器；
- 引起问题的指标；
- 探针接口名；

2) 可视化仪表，展示出现问题的指标的阀值和触发值，以及令该指标发生变化的参数的阀值和实际值

3) 图表，展示受到该问题影响的其他指标的实时数据和基线值；

4) 错误代码分布，展示引起问题的错误代码按时间的分布情况；

在上述例子中，可以看到该 Oracle 服务器的失败率在增长，分析结果表明新会话的增加与服务器失败率增长相关，图表中的红点标识了相关指标在问题发生时的触发值。当问题

在过去一小时内发生至少 3 次后，场景分析才会发出警告。

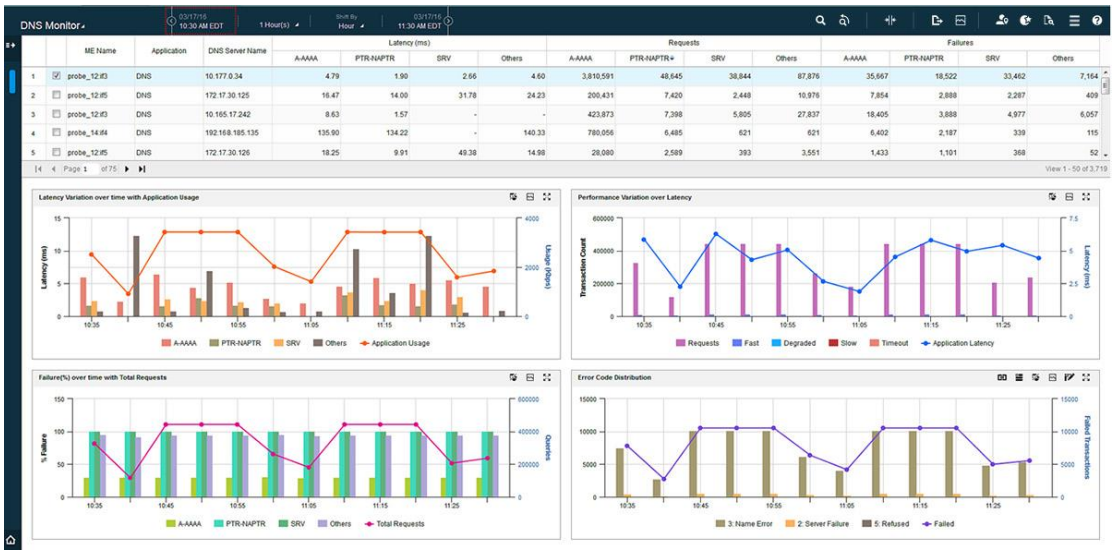
通过场景分析提供的分析报告，运维人员可以马上对交易失败率进行排查。场景分析模块为用户缩窄了排查范围，协助用户定位问题。另外用户还可以从场景分析模块直接下钻至对应的服务监测器中进行故障排查。

八、如何通过服务监测器查看应用交付质量

nGeniusONE 提供多种针对通识应用的服务监测器，帮助用户了解其应用的交付质量以及终端客户的使用体验。

例如，当用户发现 DNS 应用出现故障，可以使用 DNS 监测器去查看相关指标，从该监测器可以了解 DNS 服务对客户的体验造成什么影响。在 DNS 监测器可以查看对 DNS 的各种记录类型（如 A-AAA, PTR-NAPTR, SRV 等）的查询情况，响应情况以及查询量。

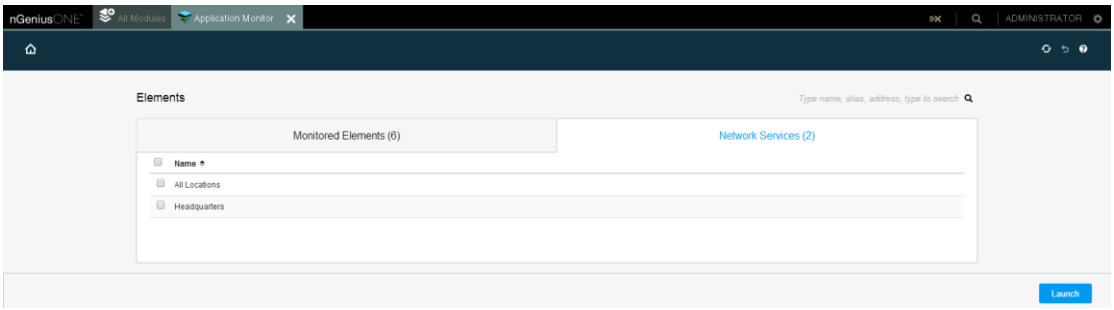
如下图，在该探针接口下的流量较高且 DNS 查询失败次数最多。在监测器中发现，“Name errors”是出现得最频繁的 DNS 错误。另外，对比界面下方四张图表结果能看出其余几张图表的曲线走势与错误代码分布基本一致，说明查询失败主要是由“Name errors”错误造成。



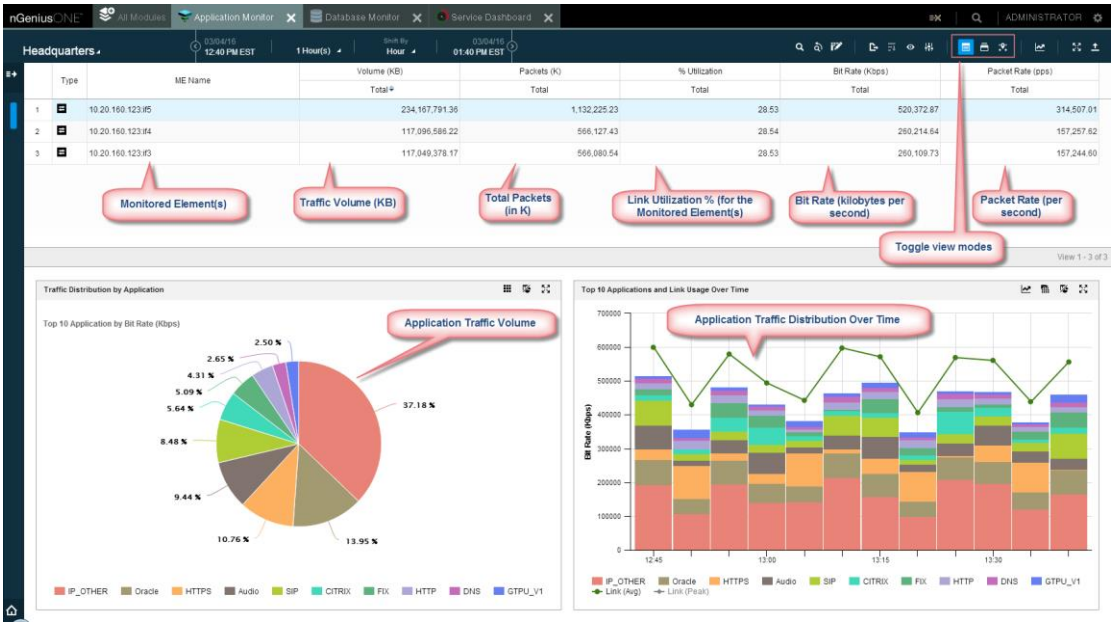
DNS 监测器中的信息能为运维人员下一步工作提供指引，如检查相关 DNS 服务器的配置。

九、如何查看链路流量中的所有应用成分

进入应用监测器  ，选中需要查看的探针接口或网络服务。

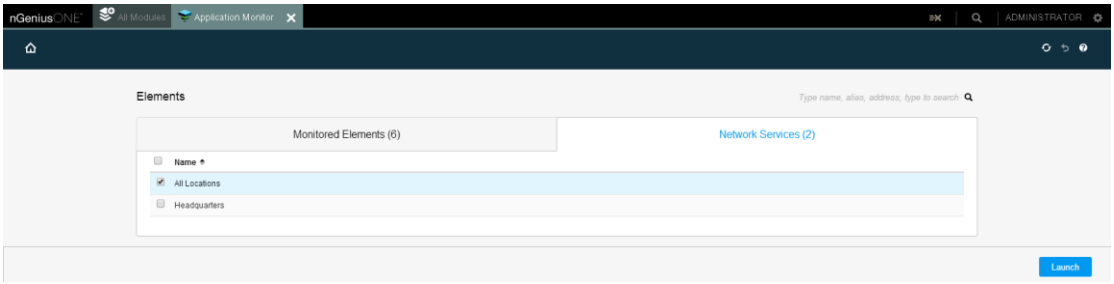


在应用监测器界面上方表格可查看总字节量、总包数以及利用率，下方图表则展示了流量前十的应用及其按时间分布的流量曲线。



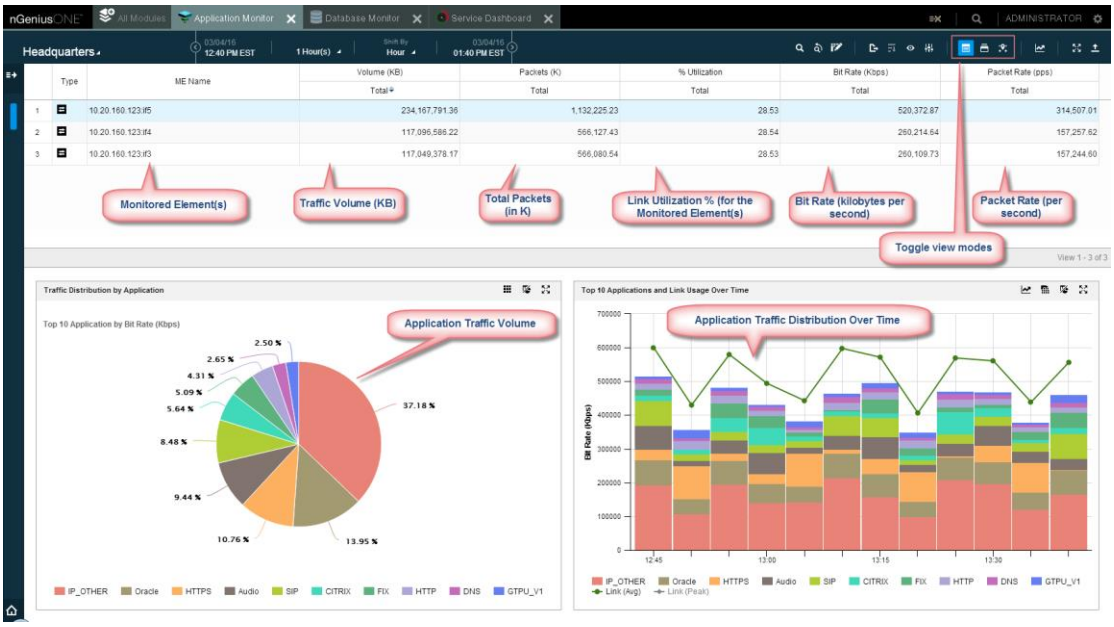
十、如何查看整个网络环境下的所有应用成分

进入应用监测器  ，选择“网络服务”→“All Locations”，然后点击运行。



在应用监测器界面上方表格可查看总字节量、总包数以及利用率，下方图表则展示了流量前十的应用及其按时间分布的流量曲线。

另外，用户可以将应用监测器的视图切换至应用模式、应用组模式和位置模式，来从不同维度了解流量中的应用成分。

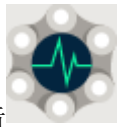


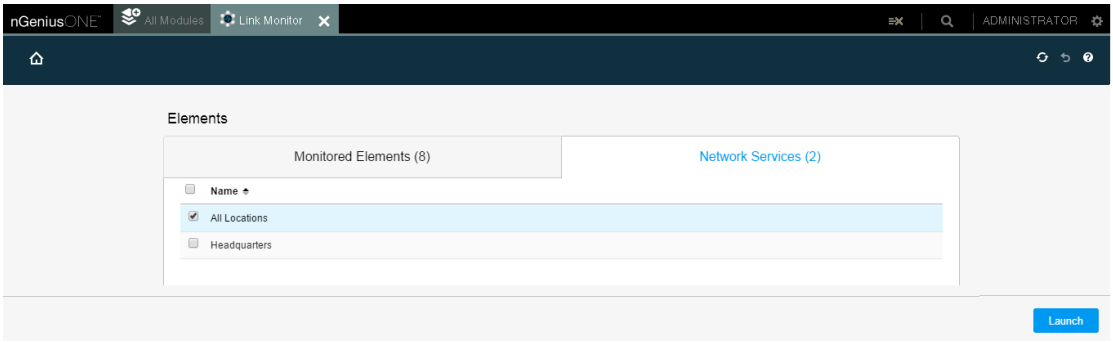
十一、 如何了解流量中的未定义应用（IP-Other）成分

用户可以用过下列方式确认和分类流量中的非通识应用成分：

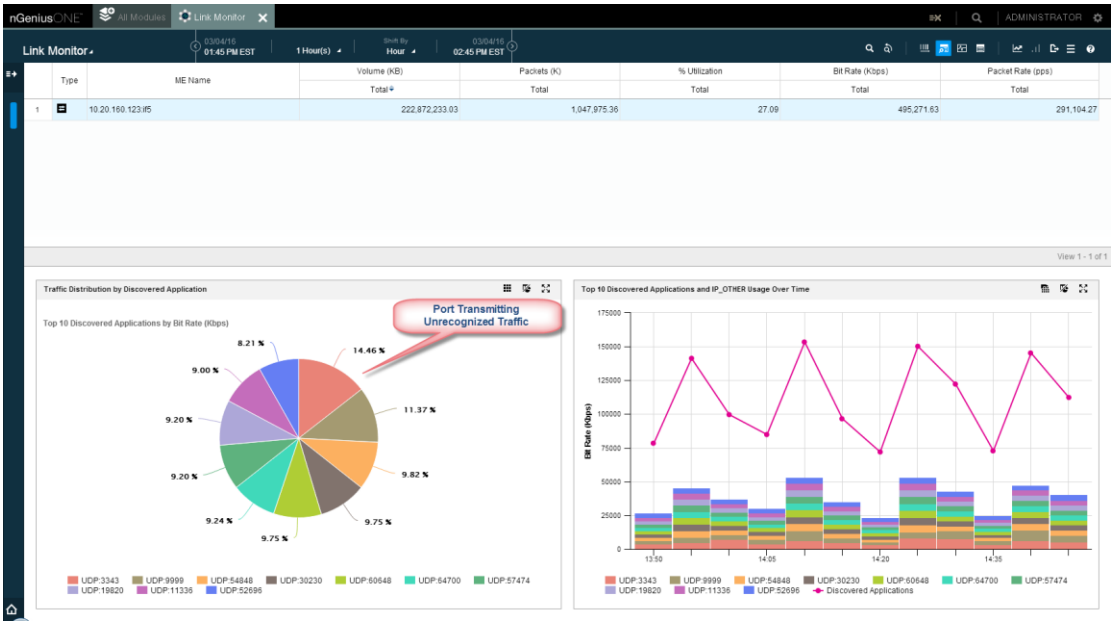
- “链路监测器”→“发现的应用”
- “链路监测器”→“发现的应用”→“协议解码”
- “全局设置”→“流量发现”

1. 链路监测器→发现的应用

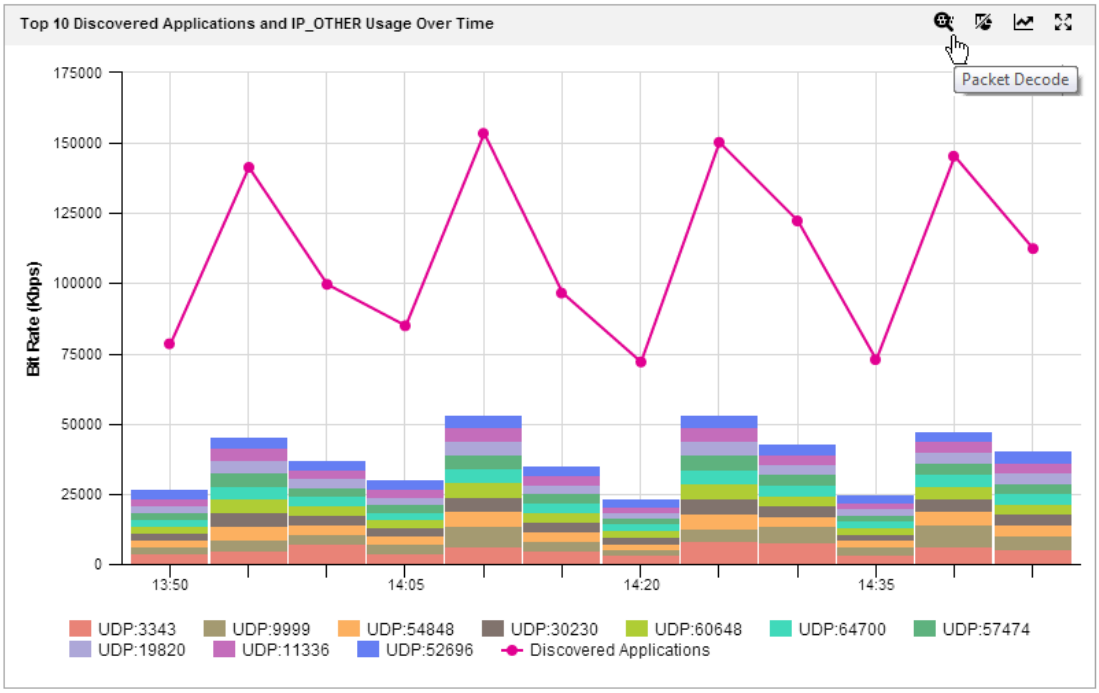
点击  图标打开链路监测器，选择“网络服务”→“All Location”，点击运行。



点击界面右上方的  按钮切换至发现的应用模式，该模式以传输层协议+端口的形式展现未匹配“全局设置”下的定义的 TCP/UDP/IP 流量（如 UDP:3343）。下方图表展示了流量前十的应用及其按时间分布的流量曲线，点击其中一个应用可以单独查看该应用的流量曲线。

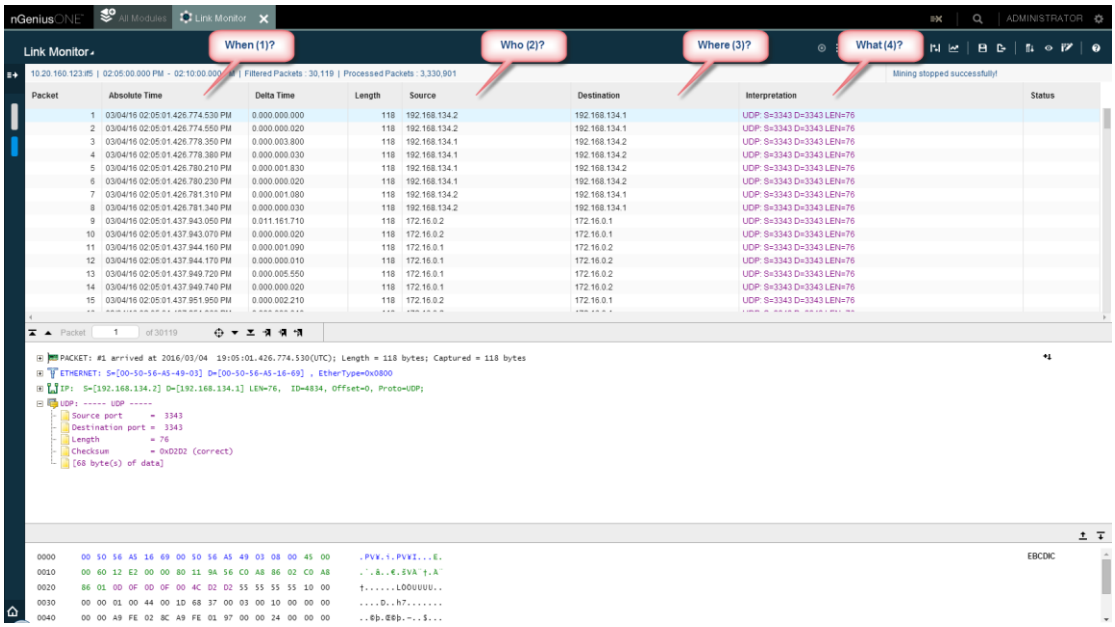


如果对某个未定义应用流量有疑问，用户可以选中该应用，然后点击  按钮下钻至数据包解码了解更多信息



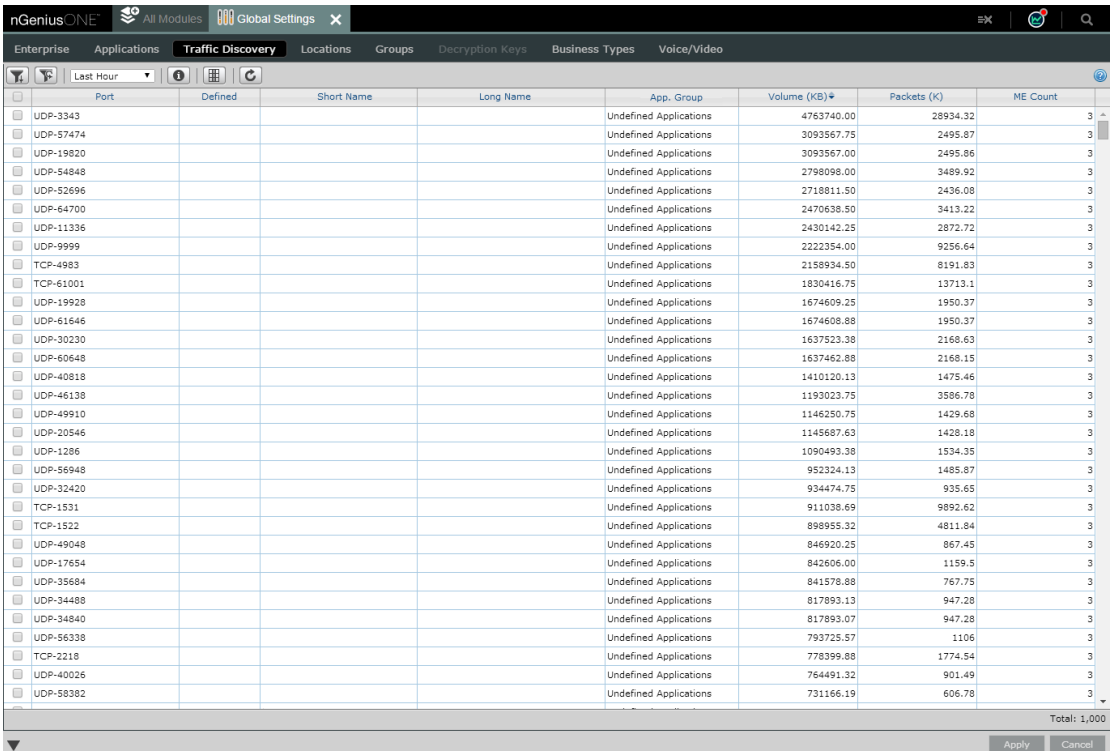
在数据包解码界面可查看以下信息：

- 数据包传输时间点
- 源目 IP 地址
- 数据包内容



2. 全局设置→流量发现

全局设置  →流量发现视图展示了所有未知的 TCP/UDP 应用流量，并且用户可以直接在该视图编辑未知流量，添加至应用定义中。



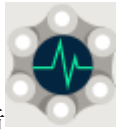
选中需要添加的未知应用后，点击应用，新增的定义会更新至数据库并同步至探针中。随后流量发现的列表会更新并排除新定义的应用。

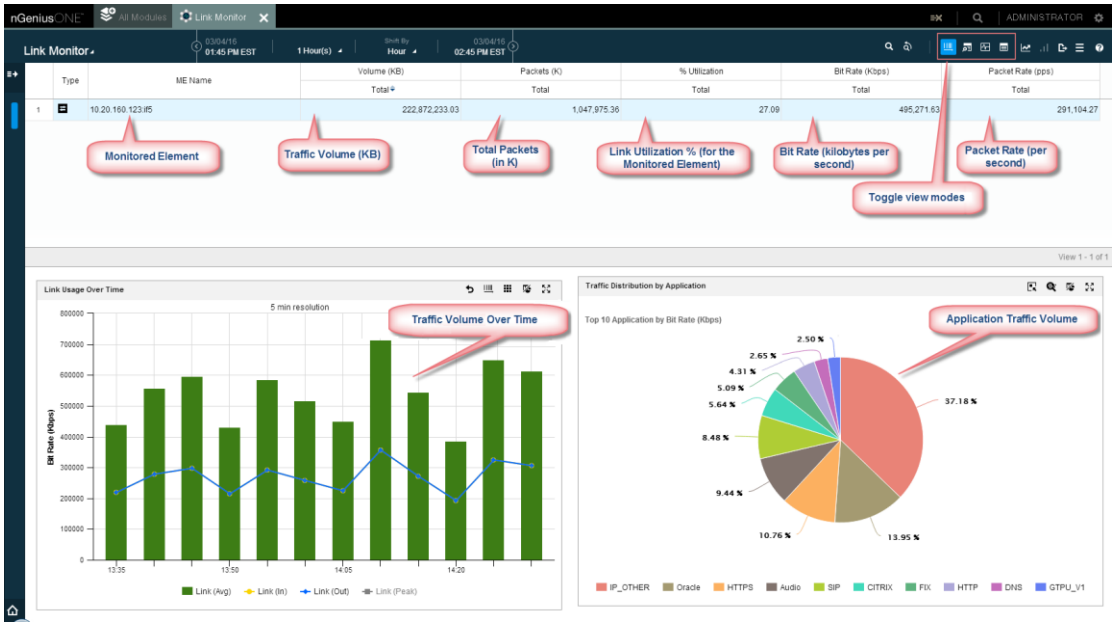
通过链路监测器的发现的应用模式，数据包解码以及流量发现，用户可以了解到流量中的未定义应用成分，产生这些流量的地址以及为这些应用添加定义和分类。

十二、 如何查看链路利用率和潜在的带宽瓶颈

了解链路的利用率有助于：

- 进行链路容量规划
- 排查网络故障
- 发现异常流量

用户可使用“链路监测器”模块查看链路利用率。点击  图标进入链路监测器，勾选要查看的探针接口或网络服务。在链路监测器界面上方表格可查看总字节量（KB）、总包数（K）以及探针所监控链路的利用率，下方图表则展示了链路流量的时间分布曲线及对应时间段流量前十的应用。



十三、 为什么要创建服务器团体和客户端团体

用户可以填入 IP 地址、地址段或 MSISDN/IMSI 电话号码来将网络中的服务器、客户端或重要业务地址定义成团体，定义后，便能对对应的关键流量进行监控。通过配置我的网络、服务器团体、客户端团体、VIP 团体可指导物理探针从 ASI 数据中过滤出具体地址或地址段的响应情况指标。

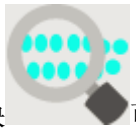
服务器团体监控填入的网段或 IP 地址中的服务器和客户端活动，而客户端团体只关注客户端，两个团体定义都可提供有利于监控应用服务的虚拟层视图视图。另外，定义在多个应用下的服务器最好定义成服务器团体，而不会作为服务器被其他地址访问的客户端地址应该定义成客户端团体。这些团体配置会反映在服务依赖性中，标识出各个团体间的访问路径，增强视图的可视化特性。

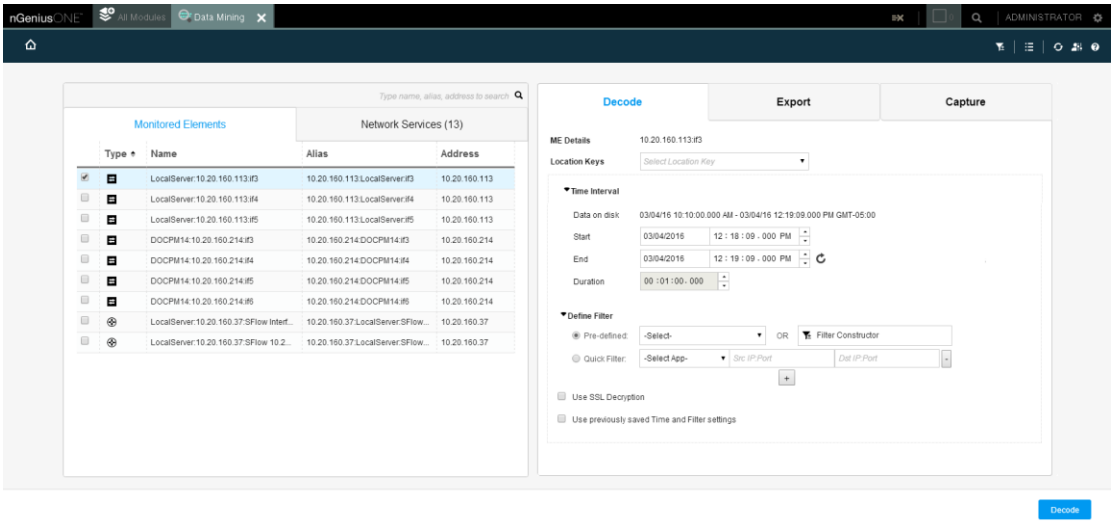
VIP 团体是一类需要特别关注的 IP，如公司 CEO 所用的 IP 地址。VIP 团体同时支持用 IP 地址和 MSISDN/IMSI 电话号码定义。

用户可以浏览 nGeniusONE Online Help 中的 Understanding Communities 文档了解更多信息。

十四、 如何通过数据包解码排查问题

对于熟悉如何通过底层数据包排查网络问题的人员，可以通过 nGeniusONE 的数据包分析模块查看原始数据包。

数据挖掘模块  可以让用户对历史数据包进行解码或导出，也可以实时捕获网络中的数据包。

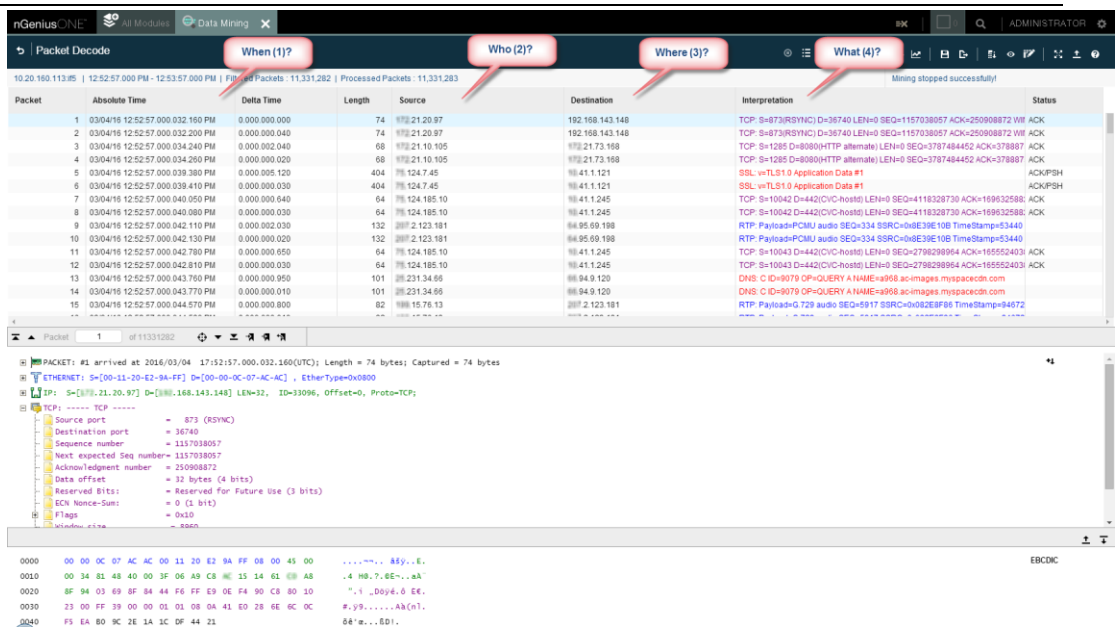


模块界面左侧列出了各个探针接口和网络服务，用户可以通过勾选其中的一项或多项进行数据挖掘操作。当选中探针接口时，用户可对该接口下的所有流量进行操作；选中网络服务时，则按照该网络服务的定义（网段、VLAN、QoS level 等）对过滤后的流量进行操作。

在左侧完成选择后，在模块界面的右侧开始操作。“解码”代表直接在 nGeniusONE 中对历史数据包进行解码；“输出”代表将历史数据包导出并保存在指定位置；“捕包”代表对实时流量进行数据包捕获。

当进行解码和捕包操作时，在右下方填入适当的过滤条件（时间、IP 地址、应用等），然后在解码窗口点击“解码”或在捕包窗口点击“开始”进行数据包操作。当操作完成后，会打开数据包解码窗口并展示以下信息：

- 数据包传输时间点
- 源目 IP 地址
- 数据包内容


nGeniusONE
All Modules
Data Mining
ADMINISTRATOR
Packet Decode
When (1)?
Who (2)?
Where (3)?
What (4)?
Mining stopped successfully!
Packet
Absolute Time
Delta Time
Length
Source
Destination
Interpretation
Status
PACKET: #1 arrived at 2016/03/04 17:52:57.000.032.160(UTC); Length = 74 bytes; Captured = 74 bytes
ETHERNET: S=[00-11-20-E2-9A-FF] D=[00-00-0C-07-AC-AC] , EtherType=0x0800
TCP: ----- TCP -----
Source port = 873 (RSYNC)
Destination port = 36740
Sequence number = 1157038057
Next expected Seq number= 1157038057
Acknowledgment number = 250908872
Data offset = 32 bytes (4 bits)
Reserved Bits: = Reserved for Future Use (3 bits)
ECN Nonce-Sum: = 0 (1 bit)
Flags = 0x10
EBCDIC