

XPM 全栈性能管理与流量分析平台

用 户 手 册

Ver 3.3

2019 年 5 月

目录

| | | |
|--------|-----------------------------|----|
| 1. | 前言..... | 11 |
| 1.1. | 概述..... | 11 |
| 1.2. | 读者对象..... | 11 |
| 2. | 安全与隐私声明..... | 12 |
| 2.1. | 安全声明..... | 12 |
| 2.1.1. | 数据管理和保护说明..... | 12 |
| 2.1.2. | 密码配置及修改的声明..... | 12 |
| 2.1.3. | 安全日志与账号权限..... | 13 |
| 2.1.4. | 流量镜像功能的免责声明..... | 13 |
| 2.2. | 隐私声明..... | 13 |
| 2.2.1. | XPM 会如何收集和使用您的个人信息..... | 14 |
| 2.2.2. | XPM 会如何使用 Cookie 和同类技术..... | 15 |
| 2.2.3. | XPM 如何共享、转让、公开披露您的个人信息..... | 16 |
| 2.2.4. | XPM 如何保护您的个人信息..... | 16 |
| 2.2.5. | 第三方链接及其产品与服务..... | 17 |
| 2.2.6. | 本声明如何更新..... | 17 |
| 2.2.7. | 如何联系我们..... | 17 |
| 3. | 名词与产品关键词解释..... | 18 |
| 3.1. | 名词解释..... | 18 |
| 3.1.1. | 什么是性能管理..... | 18 |
| 3.1.2. | KPI..... | 18 |

| | | |
|----------|-----------------------------|----|
| 3. 1. 3. | KQI..... | 18 |
| 3. 1. 4. | 旁路镜像..... | 18 |
| 3. 1. 5. | APM 和 NPM/NPMD..... | 18 |
| 3. 1. 6. | APM..... | 19 |
| 3. 1. 7. | NPM/NPMD..... | 19 |
| 3. 2. | 产品关键词解释..... | 19 |
| 3. 2. 1. | 观察点..... | 19 |
| 3. 2. 2. | 服务端..... | 19 |
| 3. 2. 3. | 客户端..... | 20 |
| 4. | 价值与应用场景..... | 21 |
| 4. 1. | 产品定位与价值..... | 21 |
| 4. 1. 1. | 产品定位：以性能指标，连接运维与业务！..... | 21 |
| 4. 1. 2. | 产品价值：是实现主动运维，高效运维的必然选择..... | 21 |
| 4. 1. 3. | 与运维大数据和 AIOPS 的关系..... | 22 |
| 4. 2. | 应用场景概述..... | 22 |
| 4. 2. 1. | 应用场景 1：性能与质量预警..... | 22 |
| 4. 2. 2. | 应用场景 2：事故责任界定..... | 22 |
| 4. 2. 3. | 应用场景 3：故障域极速定位..... | 23 |
| 4. 2. 4. | 应用场景 4：事故场景还原..... | 23 |
| 4. 2. 5. | 应用场景 5：性能优化建议..... | 24 |
| 4. 2. 6. | 应用场景 6：通信拓扑发现与梳理..... | 25 |
| 4. 2. 7. | 应用场景 7：数据库监控..... | 25 |

| | |
|---------------------------|----|
| 4.2.8. 应用场景 8：异常流量分析 | 25 |
| 5. 版本说明 | 26 |
| 5.1. XPM 的三个版本区别 | 26 |
| 6. 产品特点与优势 | 27 |
| 6.1. 无干扰，松耦合，更安全的部署方法 | 27 |
| 6.2. 全网，全业务链，全架构的监控能力 | 27 |
| 6.3. 面向监控对象和运维场景的产品设计 | 27 |
| 6.4. 高性能的实时大数据方案 | 28 |
| 6.5. 完善的服务方案，确保价值得到充分发挥 | 28 |
| 7. 产品架构 | 30 |
| 7.1. 一体化 B/S 架构 | 30 |
| 7.2. XPM-H 版本逻辑架构 | 30 |
| 7.3. XPM-S 和 XPM-V 版本逻辑架构 | 31 |
| 7.4. 虚拟机安装 XPM-V 版本 | 31 |
| 8. 产品获取与安装 | 32 |
| 8.1. 产品获取 | 32 |
| 8.2. 产品安装 | 32 |
| 9. 产品部署 | 33 |
| 9.1. XPM-S 版本的硬件要求 | 33 |
| 9.2. XPM-S 的处理性能标准 | 33 |
| 9.2.1. XPM-H 版本的硬件要求 | 33 |
| 9.2.2. 如何接入镜像流量 | 34 |
| 9.3. 如何实现对私有云内租户单元的性能监控 | 35 |

| | | |
|---------|--------------------------------------|----|
| 9.3.1. | XPM-H 或 XPM-S 版本监控不同节点机之间的虚拟机流量..... | 35 |
| 9.3.2. | XPM-V 版本监控私有云内部各虚拟机的东西向流量..... | 35 |
| 9.4. | 验证流量是否正确接入..... | 36 |
| 9.4.1. | 查看镜像流量是否接入..... | 36 |
| 9.4.2. | 是否打开 VLAN 分析设置..... | 37 |
| 9.4.3. | 设置时间服务器..... | 37 |
| 9.4.4. | 设置观察点..... | 37 |
| 9.4.5. | 验证用户提供的 IP 信息是否正确..... | 38 |
| 9.4.6. | 验证通信是否存在..... | 38 |
| 9.4.7. | 验证业务链关系是否正确..... | 39 |
| 9.5. | 流量接入的常见问题..... | 40 |
| 10. | KPI 与 KQI 说明..... | 41 |
| 10.1. | 深刻理解 KQI 和 KPI 的关系..... | 41 |
| 10.2. | XPM 的 KPI 和 KQI 都有哪些？..... | 41 |
| 10.2.1. | 网络 KPI 与 KQI..... | 41 |
| 10.2.2. | 应用层 KPI 与 KQI..... | 42 |
| 10.2.3. | 性能指标 KQI 的解释与故障域方向..... | 42 |
| 10.2.4. | KPI 与 KQI 算法说明..... | 43 |
| 11. | XPM 的四种数据格式..... | 44 |
| 11.1. | 图形化数据..... | 44 |
| 11.2. | 通信对数据..... | 44 |
| 11.3. | 应用层会话..... | 45 |
| 11.4. | 原始数据包..... | 45 |

| | |
|------------------------------|----|
| 11.5. 四种数据格式的关系..... | 45 |
| 12. 获得使用授权，激活 XPM..... | 46 |
| 12.1. 登陆系统..... | 46 |
| 12.1.1. 第一次登陆 XPM..... | 46 |
| 12.1.2. XPM 支持的浏览器种类..... | 46 |
| 12.1.3. XPM 的默认账号和密码分别是..... | 46 |
| 12.2. 获得使用授权，激活 XPM..... | 47 |
| 12.3. 授权功能页面使用说明..... | 47 |
| 13. 系统设置..... | 48 |
| 13.1. 如何进入系统设置功能..... | 48 |
| 13.2. 系统设置与管理..... | 49 |
| 13.2.1. 系统信息..... | 49 |
| 13.2.2. 管理网口设置..... | 50 |
| 13.2.3. 内网网段设置..... | 50 |
| 13.2.4. 数据包去重设置..... | 50 |
| 13.2.5. VLAN 分析设置..... | 51 |
| 13.2.6. 云端管理设置..... | 51 |
| 13.2.7. 网卡状态..... | 52 |
| 13.2.8. 系统时间设置..... | 52 |
| 13.2.9. 智能基线显示设置..... | 52 |
| 13.2.10. 邮件发送设置..... | 53 |
| 13.2.11. 企业微信发送设置..... | 53 |
| 13.2.12. 数据存储设置..... | 53 |

| | |
|--------------------------------|----|
| 13. 2. 13. 抽样比例设置..... | 54 |
| 13. 2. 14. SYSLOG 服务器设置..... | 54 |
| 13. 3. 产品更新与授权..... | 55 |
| 13. 3. 1. 配置导入与导出..... | 55 |
| 13. 3. 2. 应用配置 EXCEL 导入..... | 55 |
| 13. 3. 3. 系统升级..... | 56 |
| 13. 3. 4. 生成授权信息，上传授权文件..... | 56 |
| 13. 4. 账号管理..... | 56 |
| 13. 4. 1. 添加账号..... | 57 |
| 13. 4. 2. 账号管理的编辑，删除和修改密码..... | 58 |
| 13. 5. 系统日志..... | 58 |
| 13. 6. 系统工具..... | 58 |
| 13. 6. 1. 设备操作..... | 59 |
| 13. 6. 2. 系统资源消耗..... | 59 |
| 14. 监控对象设置..... | 61 |
| 14. 1. 监控对象种类..... | 61 |
| 14. 2. 进入监控对象设置..... | 61 |
| 14. 3. 观察点管理与设置..... | 62 |
| 14. 3. 1. 新增，编辑，删除观察点..... | 62 |
| 14. 4. 服务端管理与设置..... | 63 |
| 14. 5. 客户端管理与设置..... | 64 |
| 14. 6. HTTP 服务管理与设置..... | 64 |

| | |
|---|----|
| 14.6.1. 解析、存储 HTTP 负载段报文内容，并检索关键词..... | 64 |
| 14.7. Oracle/MySQL/SQLserver 服务管理与设置..... | 65 |
| 14.8. URL 服务管理与设置..... | 65 |
| 14.8.1. 如何监控一个多操作步骤的 URL 业务？..... | 65 |
| 14.9. 应用可用性管理与设置..... | 66 |
| 15. 告警相关功能..... | 67 |
| 15.1. 必须了解的告警算法要点..... | 67 |
| 15.2. 告警阈值设置..... | 67 |
| 15.2.1. 告警阈值设置的功能入口..... | 67 |
| 15.2.2. 如何合理的设置性能指标 KQI 的告警阈值..... | 68 |
| 15.2.3. 如何合理的设置状态指标 KPI 的告警阈值..... | 69 |
| 15.3. 告警信息获取和钻取..... | 69 |
| 15.3.1. 告警信息的获取..... | 69 |
| 15.3.2. 告警信息的钻取..... | 71 |
| 15.4. 告警统计分析功能..... | 72 |
| 15.4.1. 告警统计分析功能的入口..... | 72 |
| 15.4.2. 告警信息的字段..... | 72 |
| 15.4.3. 告警统计分析的维度..... | 73 |
| 15.4.4. 告警信息的导出..... | 73 |
| 16. 页面基础操作..... | 74 |
| 16.1. 快捷工具栏..... | 74 |
| 16.1.1. 时间回溯..... | 74 |
| 16.1.2. 刷新..... | 75 |

| | | |
|---------|----------------------------|----|
| 16.1.3. | 拓扑查询..... | 75 |
| 16.1.4. | 锁定/解锁..... | 75 |
| 16.1.5. | 全屏..... | 75 |
| 16.1.6. | 搜索查询..... | 75 |
| 16.1.7. | 帮助..... | 75 |
| 16.2. | 主要功能栏..... | 76 |
| 16.3. | 线上 IM 帮助..... | 76 |
| 16.4. | 告警信息浮动窗..... | 77 |
| 16.5. | 皮肤设置..... | 77 |
| 17. | 三种驾驶舱的功能与操作..... | 78 |
| 17.1. | 监控对象驾驶舱..... | 78 |
| 17.2. | 统计分析驾驶舱..... | 79 |
| 17.3. | 业务链驾驶舱..... | 80 |
| 17.3.1. | 如何创建一个新的业务链驾驶舱？ | 80 |
| 17.3.2. | 如何添加，修改，删除业务链驾驶舱的内容？ | 80 |
| 17.3.3. | 业务链驾驶舱搭建要点提示..... | 82 |
| 18. | 通信拓扑发现与梳理..... | 83 |
| 18.1. | 拓扑功能的基础操作..... | 83 |
| 18.1.1. | 拓扑功能的两个入口..... | 83 |
| 18.1.2. | 拓扑功能的基础操作..... | 83 |
| 18.2. | 如何使用拓扑发现功能..... | 83 |
| 18.3. | 如何使用拓扑梳理功能..... | 84 |
| 19. | 流量存储与回溯..... | 86 |

| | | |
|--------------------|-----------------------------|----|
| 19. 1. | XPM 流量存储与回溯功能的特点..... | 86 |
| 19. 2. | 流量存储的功能入口..... | 86 |
| 19. 3. | 标准存储方案..... | 87 |
| 19. 4. | 高级存储方案..... | 87 |
| 19. 5. | 历史数据提取（流量回溯）..... | 88 |
| 19. 6. | 数据提取列表..... | 88 |
| 20. | 主要功能与应用场景..... | 90 |
| 20. 1. | 对业务/应用/网络性能异常的预警和定位..... | 90 |
| 20. 2. | 性能可视化监控（上屏监控）..... | 90 |
| 20. 3. | 统计分析业务/应用/网络的运行规律与关联关系..... | 90 |
| 20. 4. | 如何定位网络串行设备的时延..... | 91 |
| 20. 5. | 如何界定用户投诉的故障域范围..... | 91 |
| 20. 6. | 对流量异常的预警和分析..... | 91 |
| 20. 7. | 如何对网络流量进行多维度分析..... | 91 |
| 20. 8. | 如何给出有针对性的优化建议..... | 92 |
| 附件 1：指标算法说明 | | 94 |
| 1. | 观察点/服务端/客户端..... | 95 |
| 2. | HTTP 服务..... | 97 |
| 3. | Oracle/MySQL/SQLserver..... | 98 |

1. 前言

1.1. 概述

本文档将详细介绍“XPM 全栈性能管理与流量分析系统”（以下简称 XPM）的功能与操作，帮助用户快速了解和掌握 XPM。

相关视频资料，还可以通过腾讯视频，搜索“XPM”而获得。

1.2. 读者对象

本文档主要适用于以下读者：

- XPM 合作伙伴的支持工程师
- XPM 的最终用户

2. 安全与隐私声明

2.1. 安全声明

2.1.1. 数据管理和保护说明

本产品的部分功能涉及用户个人或公众信息或数据，例如用户账号、密码、邮箱、电话、终端 IP 地址等。相关用户数据仅能用于本产品系统的运营、维护、故障的定位或恢复。请在正常业务需求以及在法律法规所允许的目的和范围内使用相关的功能。在使用、存储用户个人信息或数据的过程中，您应采取足够的措施，以确保用户个人信息或数据受到严格保护。包括但不限于以下内容：

- 用户管理

系统各级管理员具有很高的权限。当对应人员岗位发生变更时，应及时回收相应的权限或修改密码等，以确保用户的个人信息或数据受到严格保护。

- 数据备份

为防止数据被误修改，导致系统故障或者用户数据错误，本产品具有配置与账号信息的备份功能，用户可以定期进行备份工作。备份的内容应仅用于数据恢复，建议您遵从所在国家的相关法律执行该任务，以确保个人数据受到充分的保护，严禁将这些内容私自存储，或用作其它目的。备份到期后需要将废弃的备份数据及时删除。

- 公众信息的安全处置

对于为公众提供服务的 XPM 用户，由于您在使用 XPM 的过程中，会涉及可能敏感的公众信息，所以，我们建议您遵从所在国家的相关法律执行相关的操作，并采取足够的措施以确保用户的个人数据受到充分的保护，特别是流量回溯功能所下载的原始数据报文。

2.1.2. 密码配置及修改的声明

- 用户缺省密码在登录后请务必及时修改，并妥善保存

- 为充分保证 XPM 安全, 请您务必定期修改密码
- 为确保 XPM 的稳定性, 我们不对用户提供后台管理账号和密码

2.1.3. 安全日志与账号权限

- XPM 分为系统管理员和普通用户两个级别的账号, 系统管理员为全功能账号, 而普通用户账号是由系统管理员创建, 并赋予不同功能使用权限的账号
- 系统管理人员对账号的增删改操作均有记录
- 普通用户登录系统、注销登录日志均有记录

2.1.4. 流量镜像功能的免责声明

作为以网络流量为分析对象和基础数据的产品, XPM 无法回避使用包含有敏感信息的网络流量; 我们将按照如下方案获得用户的豁免:

- 对于已经购买 XPM 的用户, 由于设备的所有权归属用户, 因此我们将无法知晓任何用户网络流量里的敏感信息;
- 而对于对其他用户提供服务而使用的 XPM 系统, 我们只会在用户授权的情况下, 并仅限于功能自身需求而分析并了解网络流量里可能存在的敏感信息, 如果用户对此有任何担心, XPM 的服务方可以出具相关信息保密文件, 用户也可以禁止 XPM 开启可能知晓敏感信息的功能, 包括: HTTP 协议分析, SQL 协议分析, 以及流量回溯功能。

2.2. 隐私声明

XPM 产品功能及原始代码开发商深知隐私对您的重要性, 并充分尊重您的隐私权。我们特此制定本《隐私声明》(以下简称为“本声明”)以便您了解我们如何搜集、使用、披露、保护、存储及传输您的个人数据。请您仔细阅读本声明。如您有任何疑问, 请联系我们。

个人信息, 是指以电子或者其他方式记录的, 能够单独或者与其他信息结合识别自然人个人身份的各种信息。本声明阐述了华为如何处理您的个人信息, 但本声明不涵盖所有的处理场景, 本声明讨论、提及、介绍的产品或服务也并非均可由所有人或在所有地理位置获得。具体产品或服务如何处理您的个人信息由华

为在该产品或服务的专门的隐私通知或补充声明中发布。在使用具体产品或服务时，除本声明外，还建议您阅读有关隐私通知或补充声明。本声明仅适用于 XPM 系列产品。

本声明将帮助您了解以下内容：

- 一、XPM 会如何收集和使用您的个人信息
- 二、XPM 会如何使用 Cookie 和同类技术
- 三、XPM 是否会共享、转让、公开披露您的个人信息
- 四、XPM 会如何保护您的个人信息
- 五、XPM 如何管理您的个人信息
- 六、XPM 会如何处理未成年人的个人信息
- 七、第三方链接及其产品与服务
- 八、您的个人信息如何在全球范围转移
- 九、本声明如何更新
- 十、如何联系我们

2.2.1. XPM 会如何收集和使用您的个人信息

● XPM 收集的个人信息

- 您在使用 XPM 产品或服务时，可能需要提供个人或单位信息。您并非必须向 XPM 提供个人信息，但一些情况下，如果您选择不提供，我们将无法为您提供相关产品或服务，也无法回应或解决您所遇到的问题。
- 我们仅会出于本声明所述目的收集和使用您的个人信息。下文举例说明了我们可能收集的个人信息的内容和途径：
- 为获得 XPM 的使用授权，您需要向我们提供的必要的注册信息，例如，用户名称，单位名称，联系方法等；
- 此外，如果您对监控指标和监控对象的信息也视为个人信息，我们也将只有在您授权我们使用时，并上传到云端监控服务中心。

- 为了正常使用微信或告警远程通知，华为可能会收集有关的信息，如姓名、电子邮件地址以及电话号码等。华为将采取合理且必要的措施保障前述通信的安全；
- 我们将如何使用您的个人信息
 - 注册、激活您购买的 XPM 产品与服务；
 - 交付、激活或验证您所请求的产品与服务，或应您的要求对前述产品与服务进行变更、提供技术支持与售后服务；
 - 向您发送操作系统或应用程序更新和安装的通知；
 - 在您明确同意或应您主动要求，与您联系、向您发送有关您可能感兴趣的产品与服务的信息、邀请您参与华为促销活动和市场调查、或向您发送营销信息。如果您不想接收此类信息，则可以随时退订；
 - 您主动要求我们参与的数据分析工作；
 - 其他征得您同意的目的。

2.2.2. XPM 会如何使用 Cookie 和同类技术

XPM 产品和服务可能会使用 Cookie、像素标签和网站信标等本地存储技术。我们将通过 Cookie 和同类技术收集的信息视为非个人信息。但如果当地法律将 IP 地址或类似识别标记视为个人信息，则我们亦将此等识别标记视为个人信息。

- Cookie
 - 与其他基于 B/S 架构的产品一样，我们会使用 Cookie；但我们不会将 Cookie 用于本声明所述目的之外的任何用途。您可根据自己的偏好管理或删除 Cookie。有关详情，请参见 AboutCookies.org。
 - 如果您清除 Cookie，则需要在每一次使用 XPM 时亲自填写相关信息。同时也请注意，XPM 某些服务可能必须使用 Cookie，禁用 Cookie 可能会影响您使用这些服务的全部或部分功能。
- 其他本地缓存或存储
 - XPM 可能使用其他本地存储技术，例如内存中的缓存，或缓存文件，或 HTML5 本地存储。这些技术与上述的 Cookie 类似，它们同样存储在您的设备中，并且可用于记录有关您的活动和首选项

的某些信息。但这些技术与标准 Cookie 所使用的设备可能不同，因此您可能无法使用标准浏览器工具和设置来控制它们。但我们可以确认，我们对这类信息没有主动性的，有意识的获取行为，但即使如此，您如果仍需要监控此类信息的使用，则需要向浏览器的提供方进行相关管控咨询。

- Do Not Track（请勿追踪）

➤ 很多网络浏览器均设有 Do Not Track 功能，该功能可向网站发布 Do Not Track 请求。目前，主要互联网标准组织尚未设立相关政策来规定网站应如何应对此类请求。如果您的浏览器启用了 Do Not Track，那么 XPM 产品与服务都会尊重您的选择。

2.2.3. XPM 如何共享、转让、公开披露您的个人信息

- 在未经用户书面授权的情况下，在未接到必须配合的所在国执法部门的要求的前提下，我们不会授权、授意或默许任何第三方共享、转让、公开您的个人信息；
- 因违反此约定而出现的法律纠纷，我们愿承担官方机构量化的损失赔偿。

2.2.4. XPM 如何保护您的个人信息

我们重视个人信息的安全，并采取业内标准做法来保护您的个人信息，防止其遭到未经授权访问、披露、使用、修改、损坏或丢失。为此，我们特别采取了以下措施：

- 我们采取一切合理可行的措施，确保个人信息收集的最小化，不收集与达到目的无关的个人信息。我们只会在达成本声明所述目的所需的期限内保留您的个人信息，除非需要延长保留期或法律允许；
- 我们会使用加密技术确保数据传输和存储的机密性，使用受信赖的保护机制防止数据和存储数据的服务器遭到恶意攻击；
- 只有授权人员才可访问个人信息；并且依照业务需要和人员层级，控制授权人员的数量并对授权人员做到分层级的权限管理；对个人数据的访问都会被记录日志，并由管理员定期审计；
- 我们会严格甄选业务合作伙伴和服务提供商，将在个人信息保护方面的要求落实到双方的商务合同或审计、考核等活动中；
- 我们会尽力保护您的个人信息。但我们深知任何措施都无法做到无懈可击，也没有任何产品与服务、网站、数据传输、计算机系统、网络连接是绝对安全的。因此，我们还制定了严格而具有惩戒性的信息保密管理条例，以提醒任何可能或尝试接触您个人信息的个人或组织；

- 如果确实发生了使您个人信息泄漏的安全事故，我们将按照法律法规的要求，及时向您告知：安全事件的基本情况和可能的影响、我们已采取或将要采取的处置措施、您可自主防范和降低风险的建议、对您的补救措施等。我们将以邮件、短信、推送通知等方式告知您事件相关情况，难以逐一告知个人信息主体时，我们会采取合理、有效的方式发布公告。同时，我们还将按照监管部门要求，上报个人信息安全事件的处置情况。

2.2.5. 第三方链接及其产品与服务

截止到本文件发布为止，XPM 产品中，未包含任何第三方商业产品，也不包含任何第三方的链接或授权；如果在日后的版本中出现此类可能导致敏感信息泄露的途径，我们将在明显位置给予提醒，也将确保您如果不进行第三方授权，该第三方产品或代码也将无法使用。

2.2.6. 本声明如何更新

我们将保留不定时更新或修改本声明的权利。

本声明变更时，我们会通过软件更新措施给予通知，重要变更我们还会在您使用 XPM 时弹出窗口通知。

2.2.7. 如何联系我们

所有在互联网上进行下载，并提供服务的 XPM 版本，均可以通过 XPM 页面下的在线沟通窗口与我们实时通信；也可以邮件联系我们，邮箱是：tcpiplabs@outlook.com。一般情况下，我们将在三个工作日内初步回复，并尽最大努力在一个月之内解答您的疑问。

重要提示：鉴于当地法律和语言差异，当地语言版本的《隐私声明》可能与本版本有所不同。如果出现任何差异，请以当地语言版本为准。

版权所有 © TCPIPlabs Technologies Inc. 2018–2019。保留一切权利。

3. 名词与产品关键词解释

3.1. 名词解释

3.1.1. 什么是性能管理

能够对信息在产生和交互过程中的实时性、准确性、稳定性，进行异常预警，故障定位，特征分析，趋势描述的技术和产品，都属于性能管理范畴；

3.1.2. KPI

在 XPM 的技术理论中，KPI 泛指状态指标，这类指标不能衡量服务质量与业务性能，只是对监控对象在某个时间点或时间段内，某种状态的表达；例如，流量的大小，包速率的高低；

3.1.3. KQI

是对监控对象运行质量和性能的表征量，与性能管理定义相一致的解释为：能够测量监控对象对信息的产生或交互的质量的指标，例如时间、错误、响应等；

3.1.4. 旁路镜像

是大多数可网管交换机或其他网络设备，或云技术里的 OVS 的一类专有功能，专门用于将某个或某些端口的流量，复制以后再发送到另一个端口的功能，被广泛用于为各类流量分析设备提供原始流量数据。由于其并不串接在网络里，所以对网络的干扰很小，在传统环境下，只对交换机产生最高不超过 3% 的负载。

3.1.5. APM 和 NPM/NPMD

业界关于 APM 和 NPM/NPMD 的定义，多以 Gartner 的为准；但我们认为，由于 Gartner 对这两个产品类型的定义有一定的历史延续性，并且，也承认这两个技术领域存在一定的需求重叠，所以我们不建议以 Gartner 的定义作为标准。我们的定义如下：

3.1.6. APM

Application Program Performance Management，即，应用程序性能管理。原理上，APM 定义为采用 Agent 或需要用户程序授权的技术方法，可以帮助用户监控和分析应用程序的执行效率。

其最大优点在于，可以对大部分开发语言的程序，进行代码级别的性能监控；但缺点也很明显，即，由于其 Agent 程序的紧耦合特性，也导致一些兼容性，安全性等风险无法避免，因此，在某种程度上并不适合对先生系统做全天候的实时性能监控，而更适合偶尔调试，或在研发和测试部门使用；

此外，这种方法的 APM，也无法监控无法植入手写 Agent 程序的网络硬件，因此，对网络节点和设备的监控有较多盲点。

3.1.7. NPM/NPMD

基于网络流量的性能管理。请特别注意，由于 Gartner 对 NPMD 定义的误导，导致很多用户认为 NPM/NPMD 产品不能监控应用和业务的性能，这实际上是一种严重的谬误！

与 Agent 的 APM 相比，除了不能监控程序代码的执行效率外，NPM/NPMD 似乎更适合更符合绝大多数用户对性能管理的需求，其优势主要体现在：

部署和使用过程中完全的松耦合特性，确保了兼容性、安全性都毋庸置疑；

在分析应用组件（例如数据库）时，不需要用户账号和密码，更加安全和无扰；

可以对网络串行设备的性能进行监控。

简言之，由于流量分析方法的松耦合特性，基于流量分析的 PM 产品，更符合生产环境部署、使用。

3.2. 产品关键词解释

3.2.1. 观察点

即为流量镜像点，又称为采集点，捕获点。是指通过交换机或路由器等网络设备的镜像端口，将网络流量引入 XPM 设备的网口，或经过 TAP 汇聚后并打上 VLAN 标签的网络流量；

3.2.2. 服务端

是指一个或一组为某个业务提供服务的 IP 或 IP:Port，具体输入方法详见 XPM 产品内部帮助；

3. 2. 3. 客户端

是指一个或一组客户端 IP，可以是单一的主机，网元，也可以是某个分支机构的一组 IP；具体输入方法详见 XPM 产品内部帮助。

4. 价值与应用场景

4.1. 产品定位与价值

4.1.1. 产品定位：以性能指标，连接运维与业务！

长期以来，运维都是面向 IT 对象的，语言也都是 IT 范畴的，这也造成与业务的沟通和理解始终存在不对位的尴尬；

例如，业务对 IT 的要求是稳定，准确，实时，完整，这些都是用户能够感知到的指标，但 IT 运维的语言却都是链路带宽，CPU 利用率，丢包率，代码 BUG，数据库索引，这两种语言存在相关性，但也存在无法跨越的理解障碍，我们不能要求业务部门或单位领导去理解 IT 语言，因为业务是生命线，是主体价值。那么，我们就需要以业务部门听得懂的语言进行解释、翻译，并应用到具体的日常工作中。

而性能管理的第一个价值就在于，以 IT 运维和业务都听得懂的性能指标，连接运维与业务，为运维和业务搭建沟通的桥梁，创建互信的语言。

4.1.2. 产品价值：是实现主动运维，高效运维的必然选择

在整个运维领域，性能管理是最接近业务的技术领域，也是最上层的技术栈；性能管理输出的主要指标，是时间，错误，响应等直接与用户感知相关的指标，而所有的生产事故和用户投诉，实际上也都是对这些指标的一种恶化反馈，例如，访问中断，卡顿，缓慢，显示不完整，这些事故或投诉，都是性能指标的监控内容。

主动运维的目标之一，是要充分降低事故率和投诉率，在很多异常未形成事故和投诉的时候，就能够主动接收到异常信息，并以此为依据，提前对异常进行预判、排查并解决。

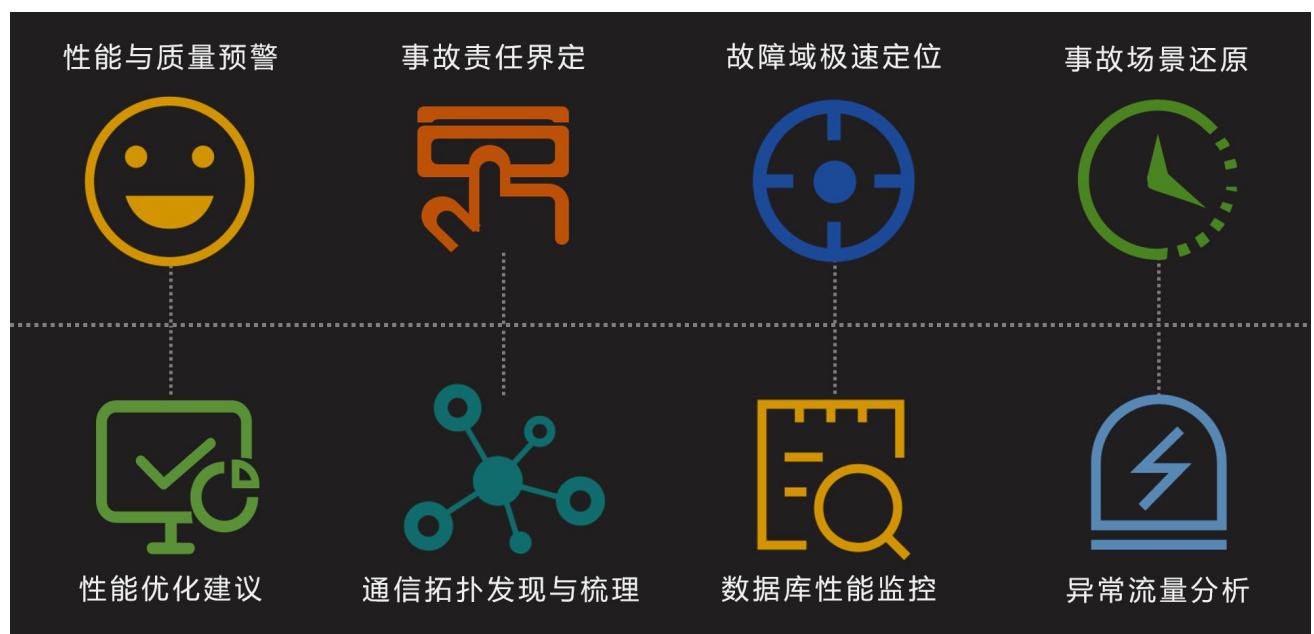
此外，在容量和资源的判断方面，性能管理的指标也是最核心，也是最为本质的参考，毫无疑问，通过性能指标的劣化趋势对容量和资源进行管理，也是最为有效，最为科学的方法。

关于高效运维，最核心的要点就是发生事故或投诉时，能够高效率的定位故障域，并排查解决故障，尽快恢复生产，在这方面作为运维领域上层建筑的性能管理，无疑也是最具有指导意义的技术类型，其对性能损耗的理解和算法，是迄今为止唯一有效的，快速定位故障域的方法论。

4.1.3. 与运维大数据和 AIOPS 的关系

近两年，运维大数据和 AIOPS 逐渐成为运维领域的方向之一，从本质上说，这两类项目大同小异，殊途同归，AIOPS 的基础就是运维大数据，而运维大数据的源数据中，最具有实用性价值的数据类型就是性能数据，没有性能数据的运维大数据和 AIOPS，就像没有检查设备帮助的医疗单位，医生和药物，都没有用武之地。

4.2. 应用场景概述



4.2.1. 应用场景 1：性能与质量预警

如前所述，每一个 IT 单元都有表征性能和质量的 KQI，这些 KQI 也都与业务和感知直接相关，成为业务质量和用户感知的组成部分。那么，只要监控这些 KQI，原则上就可以对业务质量和用户感知的异常做出早期预警，并降低事故率和投诉率。

在 XPM 的告警功能中，可以对 XPM 监控的所有对象的 KQI 进行全面的人工阈值或智能算法告警。人工阈值和智能算法告警的设置和通知，将在后面详细介绍。

如何设置告警阈值？请参见。

4.2.2. 应用场景 2：事故责任界定

在一些大中型单位中，IT 工作通常由多个相关部门组成，因此，事故发生后也经常由于无法清晰的界定责

任，而使工作安排，责任划分出现推诿扯皮的现象。

例如，某个业务的访问缓慢问题，可能与网络运维，业务运维，数据库，软件开发，甚至运营商专线有关，如果不能在事故发生后的第一时间，清晰的界定出是网络？应用？还是数据库？不仅会影响定位故障域的效率，还会影响恢复生产的时间。

如何界定事故责任？请参见。

4.2.3. 应用场景 3：故障域极速定位

在事故发生后，快速定位故障域范围，是找到根因，解决故障的重要环节。但由于与事故或投诉有关的 IT 单元很多，所以，如果没有专业方法帮助我们定位故障域，传统的基础监控和人工方法显然捉襟见肘。

- 基础监控的问题：

以 SNMP 协议为主的基础监控方案，无论是商业软件，还是开源项目，本质上都是面向设备运行状态的管理和监控，严重缺乏对性能指标 KQI。举例来说，基础监控对网络的监控方法，更像是高速公路上的检查站，收费岗，或休息区；而对于高速公路上流动的车流，却没有办法监控车速，违章，或事故，而 XPM 就像高速公路上的摄像头和智能分析系统一样，重点是监控运行在公路上的各项指标，而不是进出检查站的车流量或种类等指标。

- 手工命令的问题：

手工命令是最简单之间的方法，但也是最不可靠，最不准确的方法。可以在事故发生后，测量网络的通断，或服务的存续，以及链路的时延，但对于应用处理时延，响应，错误，以及无法复现的偶发性事故，却无能为力，更无法做到预警效果。国外的统计结果显示，只有 9% 的事故或投诉，可以通过人工命令进行分析定位，其余 87% 的事故或投诉，人工命令都无能为力。

4.2.4. 应用场景 4：事故场景还原

一些复杂的，疑难的网络运维和安全事故，能够准确、完整的还原事故发生时的各项指标，甚至原始数据包，是排障、定位和解决问题的唯一方法。在这方面，XPM 提供了丰富的数据支撑。

XPM 的三种基础数据格式：

- KPI/KQI 图形数据：

XPM 对所有所有可以实时输出的监控对象的 KPI/KQI 都提供图形化数据支持，且都可以支持不少于半年时间。因此，当某个监控对象发生异常时，用户可以通过回溯该监控对象或相关监控对象的 KPI/KQI 图形，即可找到造成监控对象异常的 KPI/KQI；

- 通信对或会话数据:

XPM 内置的数据库，会存储经过分析的每一次通信的通信对或应用层会话的五元组，应用层包头，以及该通信或会话的 KPI/KQI。因此，当某个监控对象，或 IP 发生投诉或故障时，用户可以通过查询 IP，或应用层信息（通常为 URL 或 SQL），将投诉或事故发生时的该通信或会话的各项 KPI/KQI 提取出来，提供更详细分析对象数据。

- 原始数据报文:

开启 XPM-H 的 TSE 网络流量回溯功能（XPM-S 和 XPM-V 不支持该功能），并预先设置好需要存储原始流量的各项条件，XPM 即可将符合条件的原始数据报文存储在本地服务器的磁盘阵列。当发生事故或投诉时，用户可以根据五元组信息，或通过通信对路径，从本地服务器里提取事故或投诉发生时的原始数据报文，并通过 Wireshark 等数据包离线分析工具打开，查看最为基础和详细的原始数据信息。很多时候，原始数据报文是解决疑难安全和运维事故的唯一依据，同时也是唯一证据。

4.2.5. 应用场景 5：性能优化建议

XPM 对用户网络、应用、业务有较强的优化建议能力，主要分为三个应用场景：

- 网络优化建议:

通过对服务端，客户端/分支机构的各项 KQI 进行 TOP N 排序，用户可以快速发现哪些服务端，或客户端/分支机构的性能是最差的，并且，可以通过梳理这些最差对象的通信链，发现性能瓶颈和风险，并以此为依据进行网络优化；

- HTTP 应用优化建议:

对于采用 HTTP 协议的 Web Server 和中间件，XPM 可以通过回溯一天，一周，甚至一个月的 KQI 图形，找到性能最差的时间点，并以此起点钻取到导致性能最差的 HTTP 会话和 URL；此外，通过 URL 的 TOP N 功能，也可以找到一段时间内，处理时间最长的 URL，错误返回码最多的 URL，并以此为依据进行 Web 或中间件的优化；

- 数据库 SQL 优化建议:

XPM 可以对 Oracle、SQLserver、MySQL 三大主流数据库进行细粒度的 SQL 性能监控，因此，当我们回溯数据库的 KQI 图形，并找到性能最差的时间点时，钻取就可以获得该时间点处理时间最长的 SQL；而通过 TOP 的排序功能，用户也可以对一段时间里的慢 SQL，或返回码最多的 SQL 进行定位，并以此为依据，向开发部门提出优化建议。

4.2.6. 应用场景 6：通信拓扑发现与梳理

与基础网管的基于 SNMP 协议的设备拓扑发现不同，XPM 的拓扑发现和梳理功能，完全是基于真实的，细粒度的通信对信息而生成，因此，可以有效帮助用户发现未知通信端口，发现业务链配置错误，或发现一些具有网络安全风险的主机；

关于业务链拓扑梳理，对于网络运维至关重要。之所以会产生这一需求，主要是因为业务部门在修改业务链 IP 或 Port 配置的时候，经常不主动通知网络部门，这就造成故障或投诉发生后，网络运维部门往往是基于错误的业务链进行定位和排障，大大影响了工作效率和质量。

因此，我们强烈建议，XPM 的用户要不定期的主动去梳理每个核心业务的业务链，同时，为了增加实际监控效果，还应该以梳理后的业务链去建立业务链驾驶舱，实现实时的，可以上大屏的监控效果。

4.2.7. 应用场景 7：数据库监控

之所以要单独将数据库监控模块作为一个应用场景介绍，其一，是因为数据库资产是每个用户最为核心、最为重要的资产，我们需要实时在线的性能监控方法，其二，是因为传统数据库监控方法，大多采用有干扰的方法，对数据库或多或少都存在安全性，或性能损耗的风险。例如在数据库里加载 Agent，或者，需要管理员账号和密码进行定时取数据。

但 XPM 的数据库监控模块，因为采用的是旁路流量分析方法，所以对数据库没有任何干扰，用户只需要配置数据库的 IP 即可实现对数据库的每一条 SQL 的实时分析，并实现对整体性能的预警功能，非常实用，非常易用、好用。

4.2.8. 应用场景 8：异常流量分析

虽然 XPM 是以性能管理为主的解决方案，但其基础原理仍为实时网络流量分析，因此，XPM 可以输出非常丰富的网络通信指标 KPI。这些 KPI 不仅包括流量、数据包、会话、ARP 包速率等原生 KPI，还包括了 XPM 所特有的各类比例类指标，例如，尝试连接率，连接关闭率，小包比率等。

这些 KPI 虽然与服务质量和用户感知不直接相关，但其异常却可能代表了某个安全风险，或者运维风险，因此，预警、定位、分析这些 KPI 的异常，对于运维和安全部门也至关重要。

5. 版本说明

5.1. XPM 的三个版本区别

XPM 分为三个大版本，分别是 XPM-S 和 XPM-H 和 XPM-V，其版本差别如下：

- XPM-S：标准版。适用于绝大多数用户对传统架构和 Underlay 架构的监控需求；可以部署在普通的 X86 架构服务器，甚至个人电脑，对硬件没有特别的要求；
- XPM-H：高性能版本。适用于超大型互联网用户，或电信运营商对传统架构和 Underlay 架构的监控需求；需要特定标准的硬件支持，XPM-H 的性能可以接近线速；
- XPM-V：可以部署在云环境的虚拟主机，虚拟机加载 Ubuntu Server 14 或更高的版本。可以通过 OVS 网桥的 SPAN 或 RSPAN 功能对云环境下的指定流量进行流量分析和性能监控。

| 对比项 | XPM-S | XPM-H | XPM-V |
|--------------|----------------|----------------|-------------|
| 版本名称 | 标准版 | 高性能版 | 虚拟机版 |
| 适用用户 | 绝大部分用户 | 电信运营商/大型互联网 | 私有云 |
| 交付形式 | 软件镜像 | 硬件或软件 | 软件安装包 |
| 是否包含操作系统 | √ | √ | × |
| 适用环境 | 传统架构, Underlay | 传统架构, Underlay | 私有云 Overlay |
| 网络/服务端/客户端 | √ | √ | √ |
| HTTP 模块 | √ | √ | √ |
| Oracle 模块 | √ | √ | √ |
| SQLserver 模块 | √ | √ | √ |
| MySQL 模块 | √ | √ | √ |
| URL 交易模块 | √ | √ | √ |
| 流量存储与回溯 | × | √ | × |

6. 产品特点与优势

6.1. 无干扰，松耦合，更安全的部署方法

安全、快捷、无干扰的部署方法，是用户选择运维和安全产品优先考虑的关键问题之一。

- 而 XPM 的所有监控指标和功能，均以交换机旁路镜像流量为基础实现，这种“流量复制”的方法，不仅可以确保在部署和使用过程当中不会干扰业务环境，还可以确保即使业务环境发生改变，XPM 也可以快速适配，因此，相对于 Agent 方法，拨测方法，和需要用户账号和密码的方法，旁路流量分析方法，是业界公认的最为安全，最为方便的源数据获取方法之一；

6.2. 全网，全业务链，全架构的监控能力

XPM 具备优秀的无盲点监控能力，是迄今为止业界整合度最高的一体化性能监控平台。这一优势体现在：

- 全网监控能力：

XPM 可以帮助网络运维，实现对全网范围内，各个网络节点，服务端，以及各类客户端和子网的性能监控和流量分析；在这方面 XPM 已经具备全部 NPMD 产品类型的功能和特性；

- 全业务连监控能力：

通过加载 HTTP 模块，DB 模块，URL 模块后，XPM 还可以实现对全业务链上各个应用组件，甚至每个子业务，或操作步骤的性能监控和流量分析；

- 全架构监控能力：

XPM-H 和 XPM-S 可以实现对传统架构的性能监控功能，而 XPM-V 版本，则可以部署在虚拟机环境，与 OVS 配合，实现对私有云内部租户和其他虚拟机的性能监控和流量分析。

6.3. 面向监控对象和运维场景的产品设计

XPM 的本质是流量分析软件，是数据包解析工具，但我们也知道，绝大多数这两类软件使用起来相当复杂，那么，如何才能以更低的学习成本，更低的使用难度，快速掌握 XPM 呢？面向对象去管理数据，面向场景去设计功能，无疑是最早进，最符合 XPM 本质的产品设计思路。

- 面向监控对象的功能设计：

是指如何组织管理数据，并以什么纬度呈现给用户；

与传统的数据包分析工具不同，XPM 并不是将网络流量里的各种信息和指标，都以最原始的状态呈现给用户，而是将这些信息，以 IP、port、URL 和其他特征为依据，归类到每一个监控对象，进行统计分析，并以华丽的，可定制化的前端界面，为用户呈现完整的企业级监控产品价值；

- 面向运维场景的使用逻辑：

就是要符合运维部门从宏观到微观的工作逻辑，而实践到 XPM 的设计当中，该逻辑就是从监控对象发起告警或查询开始，逐级钻取到通信对或会话，甚至离线数据包的过程。

- 简言之，无论是数据管理，还是功能逻辑，XPM 都以用户视角进行设计，严格贯彻从宏观到围观，从概要到详细的设计理念，最大限度的降低用户对 XPM 学习和使用难度。

6.4. 高性能的实时大数据方案

之所以强调高性能和实时性，是因为同类产品中，或某些开源项目中，或多或少的存在性能不够，或需要介入人工分析的现象，但显然更高的处理性能，和无人工介入的实时在线分析能力，更符合用户对一个优秀的商业产品的要求。

- 关于高性能：

最基础的理解是抓包的能力，但更真实的理解，是面对持续的网络流量，XPM 可以从抓包开始，到会话还原，到 KPI/KQI 分析，到通信对，和会话入库，每一个程序都保持极高的代码质量和处理性能，确保不会在任何一个环节，产生丢包、丢会话、丢数据，或数据错误的现象；

- 关于产品实时性：

无人工介入的实时在线处理能力，是预警各项 KPI/KQI 的基础要求，相对于某些产品还需要人工介入才能获得某些 KQI 相比，XPM 可以在无需人工参与的情况下，对几百个监控对象，几千个 KPI/KQI 进行在线的实时分析、预警、定位功能，这一特性在国内同类产品中也遥遥领先。

6.5. 完善的服务方案，确保价值得到充分发挥

作为一类较为复杂的实时大数据产品，我们相信，即使用户有时间和精力去学习它，也需要较长时间才能掌握，因此，我们需要尽力确保：在用户不会使用，或没有时间使用 XPM 的情况下，XPM 也能发挥其超越同群的功能，和丰富实用的价值。为此，我们专门设计了实用的功能和专业的服务，以避免上述情况的发生，并充分保护用户投资。

关于 XPM 的产品与方案特点，我们重点介绍了如上五点内容，因为内容较多，所以，我们再总结归纳一下，即：

- 部署安全，快速，这一点是所有流量分析原理产品的共性
- 全架构，无盲点的性能监控能力，这方面有很多 XPM 独到的优势
- 易学，易用，华丽的产品设计
- 高性能确保更高的数据准确性，用户完全可以信赖 XPM 的分析结果
- 完善的服务功能和方法，最大化的保护用户投资

7. 产品架构

7.1. 一体化 B/S 架构

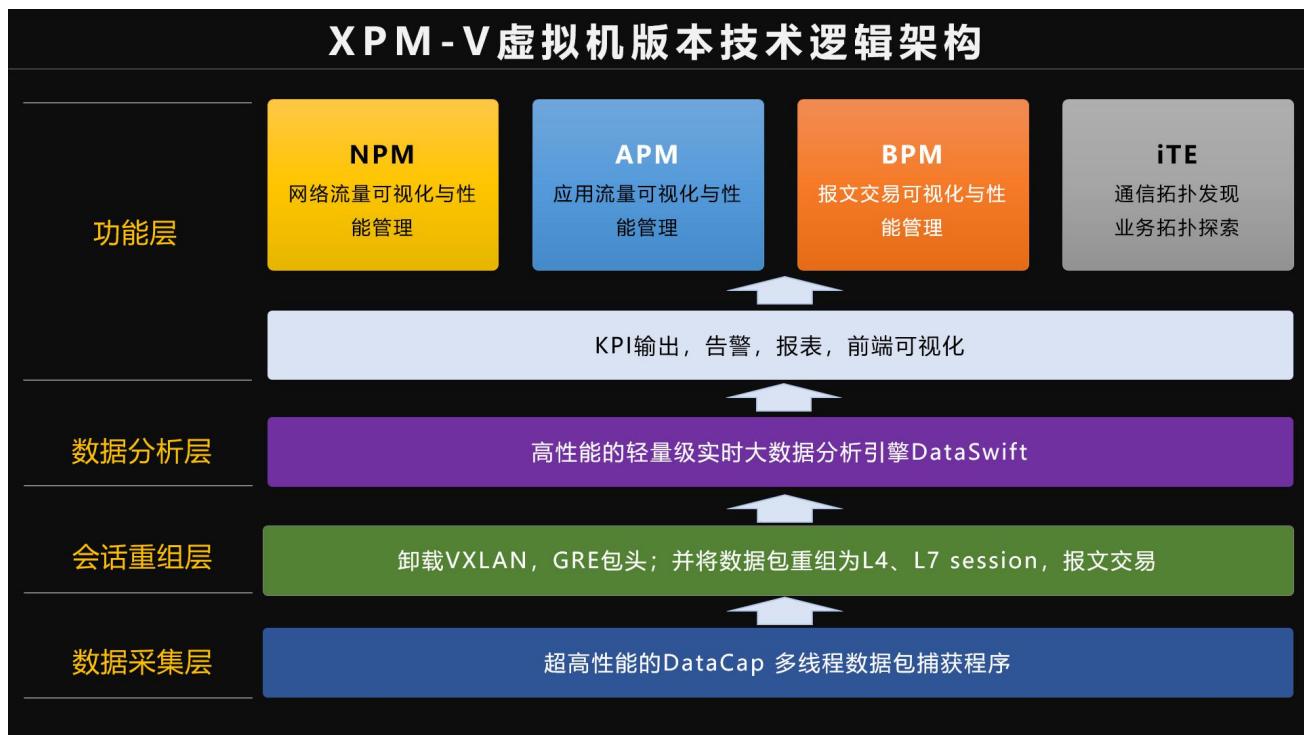
XPM 采用标准的 B/S 一体化架构，所有的程序和功能均在一个设备或一个虚拟机单元中完成。其优点在于：

- 不需要再单独部署数据采集点，分析服务器等设备，使用和部署成本都大幅降低；
- 对网络和业务的干扰降到了最低；
- 对网络质量的依赖最小，例如，当采用多层架构时，如果网络质量不好，也会导致前端数据采集服务器的数据回传到分析服务器的过程中发生丢失的情况；
- 实时性最好。因为不需要预处理，因此，XPM 前端输出的实时性可以做到 10s 刷新粒度，是业界最高的实时效率。

7.2. XPM-H 版本逻辑架构



7.3. XPM-S 和 XPM-V 版本逻辑架构



7.4. 虚拟机安装 XPM-V 版本

XPM-S 和 XPM-V 的功能基本一致，区别在于：

- XPM-S 是硬件安装，XPM-V 是云环境的虚拟机安装；
- XPM-S 提供是镜像 ISO 安装，自带操作系统；
- 而 XPM-V 是软件程序安装，需要虚拟机预装 Ubuntu Server 14 或更高版本。

8. 产品获取与安装

8.1. 产品获取

XPM 的各个版本，均可在我公司官网下载。

均可通过我公司官方渠道获得；只需要登陆我公司官方网站，注册为 XPM 用户，并通过网站的 IM 与我公司联系，即可获得相应的软件版本；

如果需要获得 XPM-H 的硬件版本，则需要与我公司或授权代理商联系，并在支付全额款项后获得。

8.2. 产品安装

会随同 XPM 的软件镜像一同提供给用户，此处不再赘述。

9. 产品部署

作为一类流量分析软件，XPM 部署方法最核心的问题，就是如何将镜像流量接入到 XPM，而镜像流量的方法在传统架构与私有云架构却存在明显的区别，因此，要有不同的软件版本和不同的方法，去适配不同的环境。关于版本选择，在这里要再次强调：

- XPM-S：标准版。适用于绝大多数用户对传统架构和 Underlay 架构的监控需求；可以部署在普通的 X86 架构服务器，甚至个人电脑，对硬件没有特别的要求；
- XPM-H：高性能版本。适用于超大型互联网用户，或电信运营商对传统架构和 Underlay 架构的监控需求；需要特定标准的硬件支持，XPM-H 的性能可以接近线速；
- XPM-V：可以部署在云环境的虚拟主机，虚拟机加载 Ubuntu Server 14 或更高的版本。可以通过 OVS 网桥的 SPAN 或 RSPAN 功能对云环境下的指定流量进行流量分析和性能监控。

9.1. XPM-S 版本的硬件要求

XPM-S 版本对硬件没有特殊要求，而且，因为 XPM-S 版本的镜像安装程序已经自带了操作系统，所以，用户只需要准备常见的标准 X86 服务器即可。以下，是 XPM-S 版以较低硬件配置实现的性能标准。

9.2. XPM-S 的处理性能标准

在如下硬件标准和流量标准的情况下，XPM 打开所有功能，可以实现稳定的，无明显因性能不足的操作卡顿。

- 硬件标准：Intel(R) Core(TM) i5-4590 CPU @ 3.30GHz 4 线程，8GB 内存，500GB SATA2 台式机硬盘；
RTL8111/8168/8411 PCI Express Gigabit Ethernet Controller
- 流量标准：网络流量≤950Mbps；TCP/UDP 会话数量≤70,000 个/秒。

9.2.1. XPM-H 版本的硬件要求

如果不加载流量回溯功能，可以参考如下标准为 XPM 配置硬件

| 配置方案 | 镜像流量 | CPU | 内存 | 磁盘阵列 | NIC |
|------|----------|-----------|------|-----------------------|------|
| 1 | <200Mbps | ≥i5 4C | 8GB | 1T*2, RAID 0, 1, 5, 6 | 2*GE |
| 2 | <500Mbps | ≥E3 V4 4C | 16GB | 1T*4, RAID 0, 1, 5, 6 | 2*GE |

| | | | | | |
|---|---------|------------|------|------------------------|--------------|
| 3 | <1Gbps | ≥E3 V4 4C | 32GB | 1T*4, RAID 0, 1, 5, 6 | 2*GE, 2*10GE |
| 4 | <2Gbps | ≥E5 V4 12C | 32GB | 1T*8, RAID 0, 1, 5, 6 | 2*GE, 2*10GE |
| 5 | <5Gbps | ≥E5 V4 12C | 64GB | 1T*12, RAID 0, 1, 5, 6 | 2*GE, 2*10GE |
| 6 | <10Gbps | ≥E5 V4 16C | 64GB | 1T*18, RAID 0, 1, 5, 6 | 2*GE, 2*10GE |

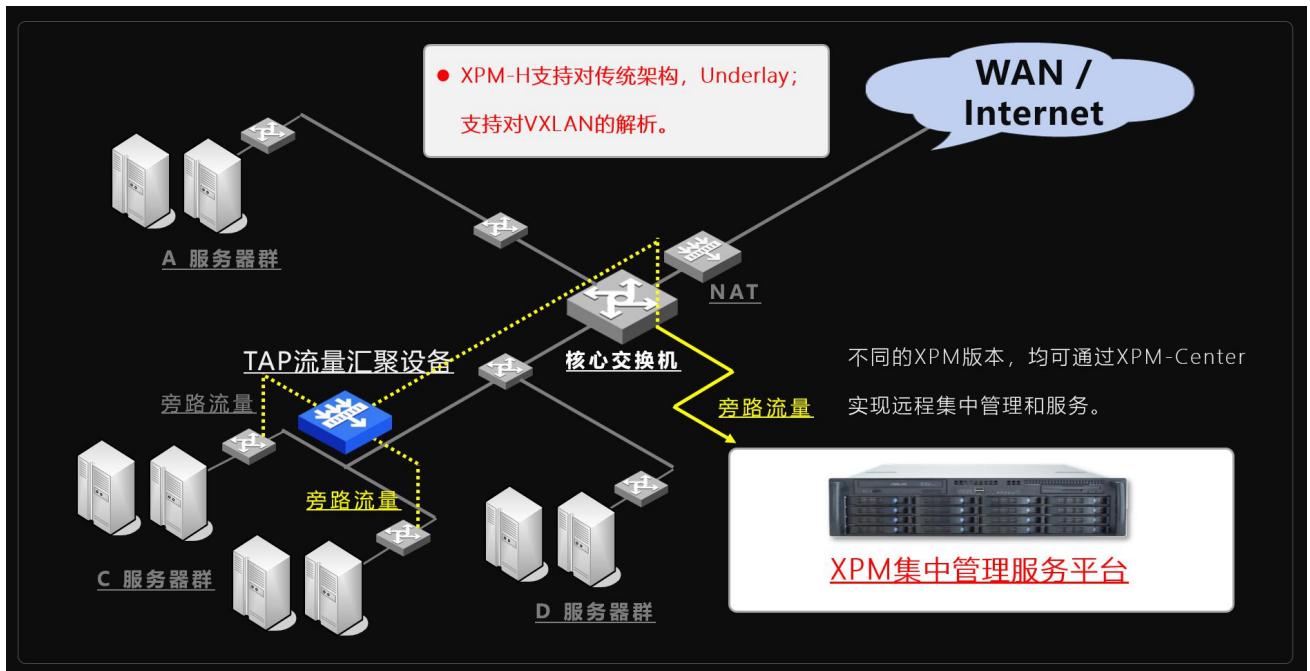
- 内存和硬盘标准需为企业级/服务器级，不建议用个人电脑级别的硬件；
- 如果加载流量回溯功能，则以上参数中的硬盘数量建议增加一倍；
- 网卡需要符合如下标准。

| 种类 | 驱动 | 主芯片 |
|---|--------|---------|
| 千兆 | e1000e | 82574L |
| | | 82571EB |
| | | 82579LM |
| | igb | I350 |
| 万兆 | ixgbe | 82599ES |
| XPM 系统，不支持万兆和千兆同时作为工作网口，但工作口是万兆，管理口是千兆可以。 | | |

9.2.2. 如何接入镜像流量

传统架构下的流量镜像较为简单，但仍然需要注意以下几点：

- 根据监控目标选择需要镜像的交换机，例如，如果需要监控 ERP 业务链的性能，则需要将 ERP 业务的各个应用组件的流量都接入 XPM；
- 如果有东西向流量需要被监控，则需要将交换机下行端口的东西向流量的端口接入 XPM；
- 如果交换机有双机热备结构，则务必注意要将两台交换机的流量都引入 XPM；
- 如果需要接入的端口比较多，还需要特别注意，镜像口是否有流量超载的情况；
- 如果有流量因地理位置无法接入 XPM，或者镜像流量很多，超过了 XPM 的网卡数量，可采用 TAP 流量汇聚设备，通过 TAP 设备给不同的镜像流量打 VLAN 标签，XPM 会根据 VLAN 标签识别不同的网络流量；
- 当部署了多台 XPM 时，可以定义某个 XPM 为主监控设备，由该 XPM 设备对其他 XPM 进行管理和监控。



9.3. 如何实现对私有云内租户单元的性能监控

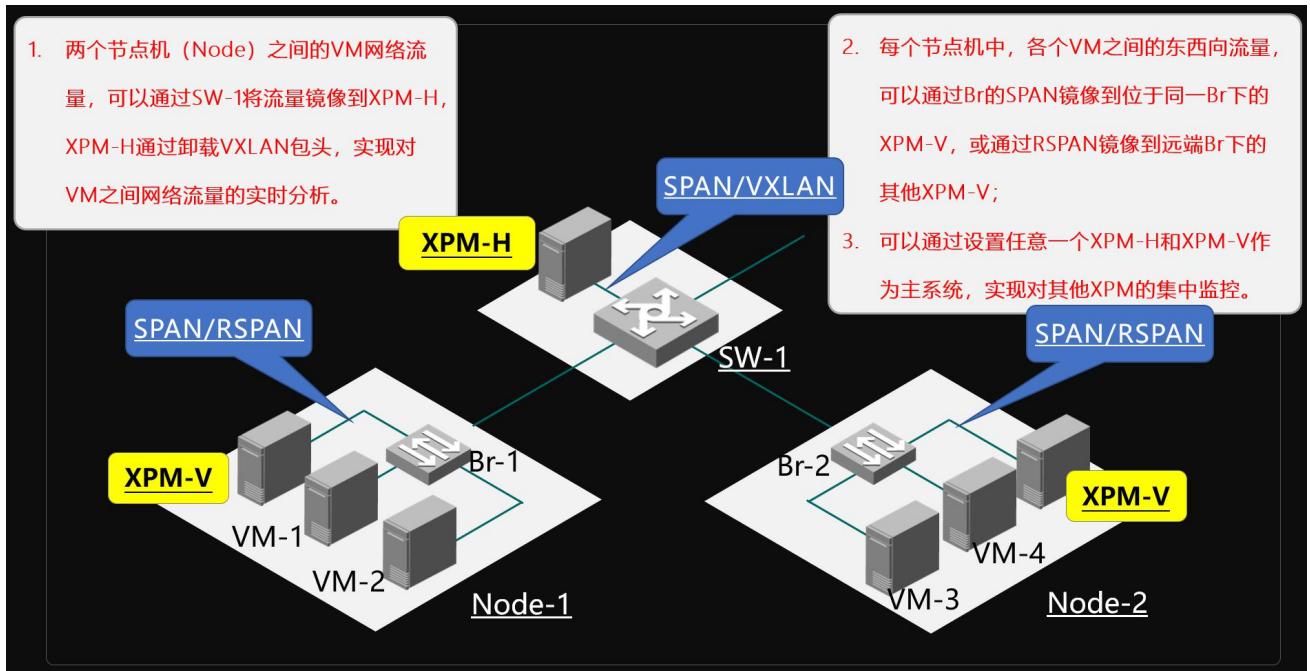
监控私有云的南北向流量，可以采用 6.1 章节的部署方法，但对于私有云内部的东西向流量，则需要按照如下方法进行部署和监控。

9.3.1. XPM-H 或 XPM-S 版本监控不同节点机之间的虚拟机流量

将安装有 XPM-H 版本的服务器，部署在连接节点机的物理交换机旁路，并将物理交换机的网络流量惊喜镜像给 XPM-H，XPM-H 即可对经过物理交换机的，虚拟机的流量进行流量分析和性能监控。这些流量的有效部分为经过 VXLAN 封装的 UDP 流量，XPM 可以解析此类流量。

9.3.2. XPM-V 版本监控私有云内部各虚拟机的东西向流量

- 节点机中各个 VM 之间的東西向流量，可以通过 Br 的 SPAN 镜像功能，接入到位于同一 Br 下的 XPM-V，或通过 RSPAN 镜像到远端 Br 下的其他 XPM-V；但考虑到流量传输过程中对私有云环境的影响，建议尽量少的采用 RSPAN，而采用部署更多的 XPM-V，结合 SPAN 的方法；
- 部署了多个 XPM-V 后，可以通过设置任意一个 XPM-H，XPM-S 和 XPM-V 作为主系统，实现对各个 XPM 版本的统一管理和呈现。



9.4. 验证流量是否正确接入

9.4.1. 查看镜像流量是否接入

路径: 【系统设置】→【系统设置与管理】→【网卡状态】; 界面如下图:

| 网卡 | IP地址 | 接收数据包数 | 接收字节数 |
|--------|----------------|---------------|-----------------|
| p261p1 | | 9908725 | 1374008778 |
| p261p2 | | 2850100995045 | 921703376079598 |
| em1 | 175.102.15.166 | 105202825 | 16380904577 |
| em2 | | 0 | 0 |

- 接收网络镜像流量的网卡，没有 IP 地址；有 IP 的是管理网卡；
- 观察没有 IP 地址的网卡的接收数据包数量，接收字节数量；流量和数据包数量明显很大的，即为工作网卡，反之则是空闲网卡；
- 记住这个有流量，但没有 IP 的网卡名称，下面，我们需要在观察点设置里面用到这个网卡名称。
- 如果所有没有 IP 的网卡的流量，都没有管理网卡大，就说明镜像流量并没有接入，需要重新排查流量是否正确接入。

9.4.2. 是否打开 VLAN 分析设置

如果采用了流量汇聚设备做流量汇聚，并且，对不同镜像流量进行了打 VLAN 标签的设置，以区分不同镜像流量，还需要开启 VLAN 标签识别功能；

- 路径：【系统设置】→【系统设置与管理】→【VLAN 分析设置】，页面如下图：



- 操作：选择【开启分析】，并点击确认。

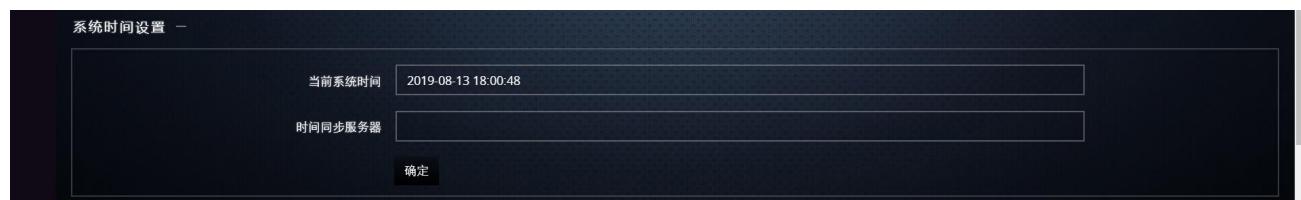
9.4.3. 设置时间服务器

- 查看 XPM 的系统时间，与用户电脑的时间是否一致；XPM 的系统时间在页面右上角，如下图：



如果 XPM 系统时间与用户电脑时间不一致，请务必给予确认；

- 如果用户内网有时间服务器，还需要在 XPM 里设置与该时间服务器的时间同步；
- 路径：【系统设置】→【系统设置与管理】→【系统时间设置】，页面如下图：



9.4.4. 设置观察点

路径：【首页】→右侧第 2 个功能→【监控对象设置】→【观察点管理与设置】→点击列表右上角【+】的【新增】，即可弹出如下窗口：

新增

| | |
|--|--------------------------|
| 名称 | <input type="text"/> |
| 网卡名 | <input type="text"/> 请选择 |
| VLAN ID | <input type="text"/> 请选择 |
| VXLAN ID | <input type="text"/> 请选择 |
| MPLS LABEL1 | <input type="text"/> 请选择 |
| MPLS LABEL2 | <input type="text"/> 请选择 |
| MPLS LABEL3 | <input type="text"/> 请选择 |
| MPLS LABEL4 | <input type="text"/> 请选择 |
| MPLS LABEL5 | <input type="text"/> 请选择 |
| 上行带宽[Mb] | <input type="text"/> |
| 下行带宽[Mb] | <input type="text"/> |
| <input type="checkbox"/> 重新开始分析 | |
| <small>此次操作需要重启分析程序，如果您需要继续修改其他同类设置，可以最后一个修改完成后，再勾选“重启分析程序”。</small> | |
| <input type="button" value="确定"/> <input type="button" value="取消"/> | |

- 在第 2 项【网卡名】，选择我们记录下的有较大网络流量的工作网卡；
- 如果有流量汇聚设备对不同镜像流量进行了打 VLAN 标签的设置，还需要选择第 3 项【VLAN ID】；
- 【上行带宽】和【下行带宽】，是镜像流量的带宽，用来输出带宽占用率；
- 添加或修改观察点，需要重启分析程序，因此，如果有多个观察点要设置，可以在都设置完成后，再选择【重新开始分析】的勾选框；如果只有一个观察点，请立即选择【重启开始分析】的勾选框。

9.4.5. 验证用户提供的 IP 信息是否正确

在进行监控对象设置前，一定要先对用户提供的 IP 信息的真实性、准确性进行验证！有两个验证方法。

9.4.6. 验证通信是否存在

路径：在页面上部的【快捷工具栏】→【搜索查询】→【服务端】，输入客户提供的某些 IP 信息，点击

确定；如下图：

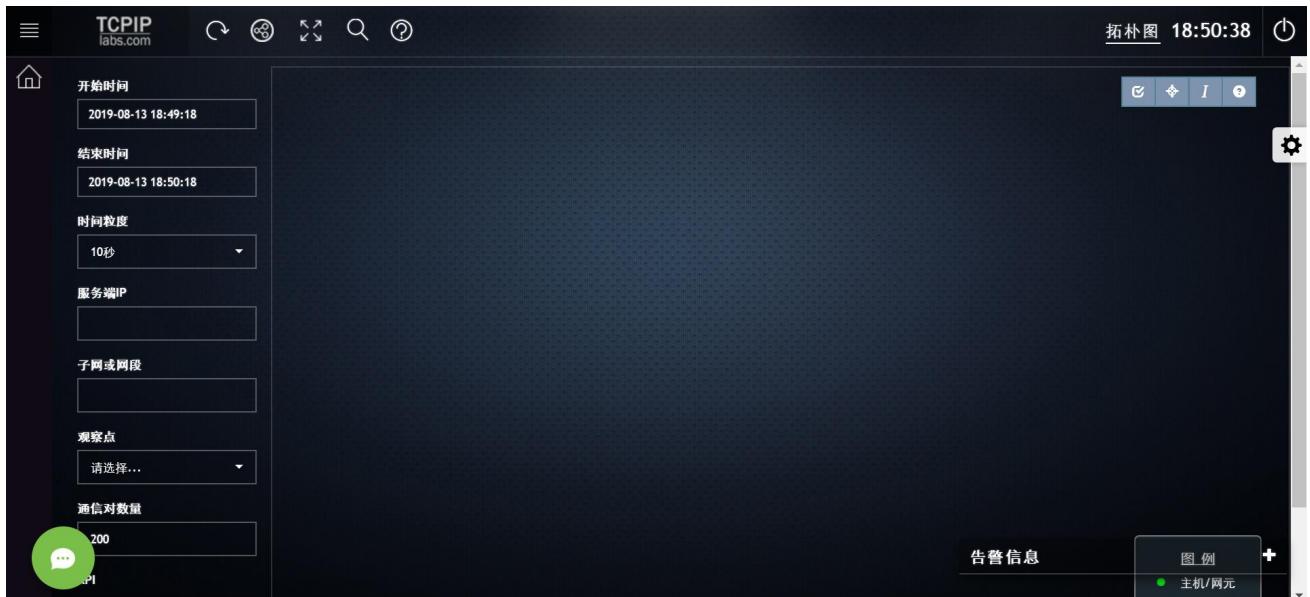


XPM 会输出包含有该 IP 的通信对，如果没有输出，说明该 IP 没有通信，或用户提供的 IP 是错误的；功能如下图：

| 发起时间 | 服务端IP | 客户端IP | 网络流量 | 连接发起数量 |
|----------------|-------------|--------------|--------|--------|
| 08-13 18:31:40 | 172.18.16.1 | 172.17.0.101 | 3.71Mb | 206 |
| 08-13 18:36:10 | 172.18.16.1 | 172.17.0.101 | 3.61Mb | 185 |
| 08-13 18:29:10 | 172.18.16.1 | 172.17.0.101 | 3.47Mb | 190 |
| 08-13 18:36:20 | 172.18.16.1 | 172.17.0.101 | 3.32Mb | 186 |
| 08-13 18:29:00 | 172.18.16.1 | 172.17.0.101 | 3.30Mb | 175 |
| 08-13 18:34:00 | 172.18.16.1 | 172.17.0.101 | 3.29Mb | 166 |

9.4.7. 验证业务链关系是否正确

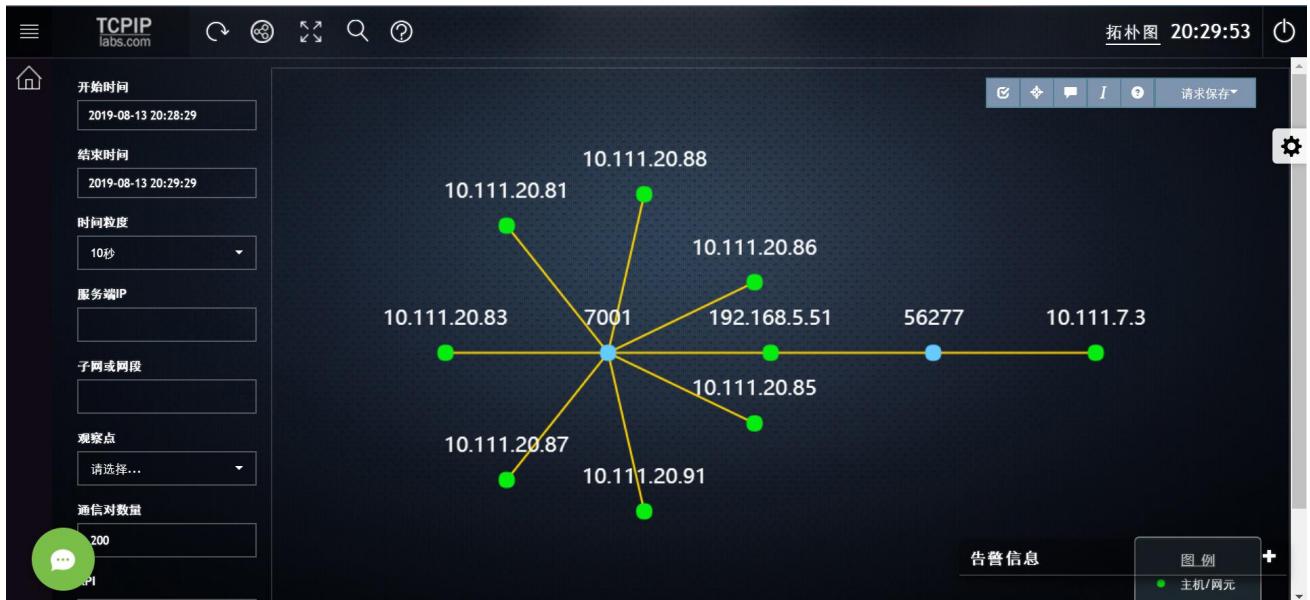
路径：在页面上部的【快捷工具栏】→【拓扑查询】，会跳转到如下图页面：



- 在左侧输入框内，按照条件输入时间，IP 等信息，即可输出该 IP 的通信逻辑；注意：要打开显示 IP（在空白处右上角的蓝色背景工具栏中）；
- 图形中，绿色圆点为 IP，蓝色为 Port；双击绿色或蓝色圆点，系统会自动为用户梳理出与之通信的下

一个 IP 和 Port;

- 通过对比这一组通信关系，与用户或业务部门提供的 IP 信息，即可找到错误或不完整的通信关系。



9.5. 流量接入的常见问题

如果发生在 XPM 里没有看到流量接入，或没有应该出现的 IP 流量，或流量镜像不完整的情况，请从如下几点找原因：

- 如果有东西向流量需要被监控，则需要将交换机下行端口的东西向流量的端口接入 XPM；
- 如果交换机有双机热备结构，则务必注意要将两台交换机的流量都引入 XPM；
- 如果需要接入的端口比较多，还需要特别注意，镜像口是否有流量超载的情况；
- 接入的流量超过网卡带宽；
- 接入的流量超过申请授权时填写的带宽；
- 需要查找的流量，是由隧道协议封装，例如 VXLAN, MPLS 等。

10. KPI 与 KQI 说明

10.1. 深刻理解 KQI 和 KPI 的关系

- 每个 KQI，都与若干个 KPI 有特定的因果关系，这些关系，也是预警和定位的基础理论之一；
- 不同单位的 IT 架构中，KQI 和 KPI 的关联性敏感度（容忍度）不同，健康的 IT 架构，KQI 对 KPI 异常的越不敏感越好（容忍度越高越好），反之则越不好；即：KQI 的异常一定是因为 KPI，而某个 KPI 劣化并不一定会影响相关的 KQI；因此，某个 KPI 的异常，并不一定形成事故和投诉，同时，由于 KPI 太多，所以将有限的精力和资源投放到成千上万的 KPI 分析中，则是一种费力不讨好的逻辑混乱，效果往往欠佳；这也是很多单位部署了庞大的开源监控项目后，运维工作仍然被动的原因之一；
- 既然，业务的事故和用户的投诉都是基于 KQI 的，那么，准确测量每个 IT 单元的 KQI，原则上就可以实现精确的事故预警和快速的故障域定位；
- 但要做到长期的预测，以及根因的挖掘，还需要精确的找到找到特定 IT 架构中，特定 KQI 和特定 KPI 之间必然的规律性关系，这也是现阶段运维大数据和未来 AIOPS 的基础目标之一。

综上所述，建立清晰的以 KQI 为指导的运维体系，是形成主动运维，高效运维的核心思想之一。

10.2. XPM 的 KPI 和 KQI 都有哪些？

10.2.1. 网络 KPI 与 KQI

| 流量 KPI | 数据包 KPI | 连接与会话 KPI | 性能类 KQI |
|---------------|------------|-----------|-------------|
| 流量/进流量/出流量 | 包速率 | 会话量 | 负载传输时长 |
| TCP 流量/UDP 流量 | 丢包率 | TCP 会话量 | 应用处理时延 |
| 未定义服务端流量 | 服务端/客户端丢包率 | UDP 会话量 | 服务端/客户端通信时延 |
| 未定义用户端流量 | 进包速率 | 会话中断数量 | 服务端/客户端握手时延 |
| 已定义服务端流量分布 | 出包速率 | 尝试连接数量 | 服务端/客户端重传耗时 |
| 已定义用户端流量分布 | 包大小分布 | 关闭连接数量 | 连接中断率 |
| 上下行带宽占用率 | 小包比率 | 尝试连接率 | 连接响应率 |
| ARP 包速率 | | 关闭连接率 | |

| | | | |
|--------|--|-------|--|
| ARP 流量 | | 会话中断率 | |
|--------|--|-------|--|

10.2.2. 应用层 KPI 与 KQI

| Web/APP | 数据库 | HTTP 中间件 | 自定义协议 | URL 业务交易 |
|-------------|----------|-------------|--------|-------------|
| URL 内容 | SQL 语句 | URL 内容 | 应用层内容 | URL 内容 |
| 流量/会话量 | 流量/会话量 | 流量/会话量 | 流量/会话量 | 流量/会话量 |
| 400/500 错误率 | 返回码错误率 | 400/500 错误率 | 中断率 | 400/500 错误率 |
| 未响应率 | 未响应率 | 未响应率 | 未响应率 | 未响应率 |
| URL 加载时延 | SQL 处理时延 | URL 加载时延 | 应用处理时延 | URL 加载时延 |
| 客户端时延 | 客户端时延 | 客户端时延 | 客户端时延 | 客户端时延 |
| 服务端时延 | 服务端时延 | 服务端时延 | 服务端时延 | 服务端时延 |
| 网络通信时延 | 网络通信时延 | 网络通信时延 | 网络通信时延 | 网络通信时延 |
| Web 处理时延 | | Web 处理时延 | | Web 处理时延 |

10.2.3. 性能指标 KQI 的解释与故障域方向

| 监控对象 | KQI 名称 | KQI 解释 | 主要故障域方向 |
|------------------------------|-------------|--------------------------|---------------|
| 网络链路 网络设备 服务群组 分支机构 | 应用响应时延 | 应用程序处理耗时, 泛指所有的应用和服务 | 应用程序 |
| | 服务端/客户端链路时延 | 以 XPM 为中点, 客户端/服务端网络链路时延 | 网络, 或网络设备 |
| | 服务端/客户端握手时延 | 客户端/服务端主机协议栈建链时延 | 主机, 或操作系统 |
| | 负载传输时延 | 负载数据的传输时延, 通常因字节量而不同 | 根据字节量判断, 是否正常 |
| | 连接重置率 | TCP 连接被中断的比率 | NAT 设备, 或操作系统 |
| | 连接未响应率 | 客户端的 TCP 连接为被服务端确认 | NAT 设备, 或操作系统 |
| HTTP 协议的应用 | Web 处理时延 | Web 服务器处理 HTTP 会话请求的 | Web 应用程序 |

| | | | |
|------------------------------|--------------|---------------------------|--------------------|
| 用 Web 中间件 | | 耗时 | |
| | HTTP 未响应比率 | HTTP 会话客户端未收到返回码的比率 | Web 服务, 或通信中断 |
| | HTTP 错误返回码比率 | 400/500 错误在所有 HTTP 会话里的比例 | Web 应用程序, 或 Web 服务 |
| Oracle SQLserver MySQL | SQL 处理时延 | DB 处理每条 SQL 的耗时 | 特定 SQL 语句, 或数据库服务 |
| | SQL 未响应比率 | SQL 会话客户端未收到返回码的比率 | 数据库服务, 或通信中断 |
| | SQL 返回码比率 | SQL 返回码不为 0 的 SQL 语句比率 | 数据库服务, 特定 SQL 语句 |

10.2.4. KPI 与 KQI 算法说明

详见附件 2。

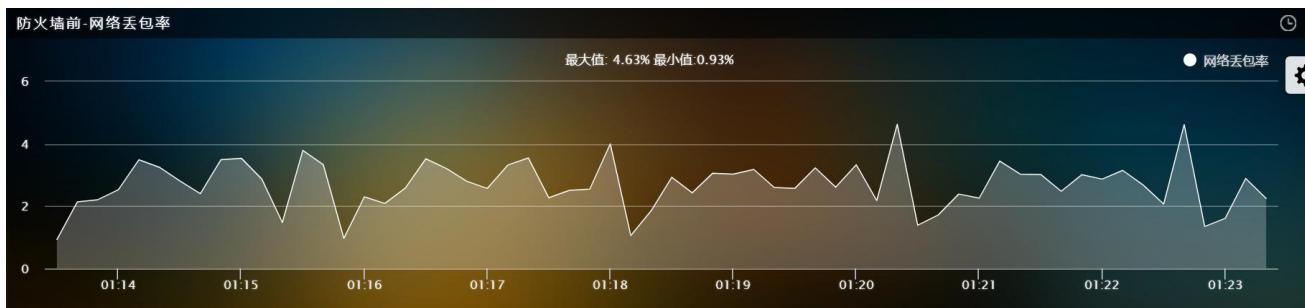
11. XPM 的四种数据格式

11.1. 图形化数据

用户在 XPM 中设置的各个监控对象的所有 KPI/KQI，都有相应的图形化数据，用来作为监控可视化和告警阈值算法的用途；其存储策略为：

- 10s 粒度，存储时间长度 4h
- 1m 粒度，存储时间长度 1d
- 10m 粒度，存储时间长度 7d
- 1h 粒度，存储时间长度 1y

用户通过回溯功能回溯图形化数据时，默认选择与回溯时间最匹配的最小时间粒度；图形化数据举例如下：



11.2. 通信对数据

对于 TCP/UDP 会话，XPM 采用聚合方法进行存储，即，每 10s 钟内客户端 IP 与 IP:Port 相同的服务端所有 TCP/UDP 通信，都会被聚合为一条记录，存储到本地数据库；记录内容包括服务端 IP:Port，客户端 IP；以及如 9.2.1 内容的 KPI 和 KQI；例如：

| | | | | | | | | | |
|---------------|----|---------------|----------|---|---------|--------|---------|------|------|
| 172.26.201.1 | 80 | 172.26.25.11 | 19.06Kb | 0 | <1ms | <1ms | <1ms | <1ms | <1ms |
| 172.26.201.3 | 80 | 155.1.120.2 | 14.46Kb | 0 | <1ms | <1ms | <1ms | <1ms | <1ms |
| 172.26.201.3 | 80 | 155.1.120.4 | 38.70Kb | 0 | <1ms | <1ms | <1ms | <1ms | <1ms |
| 172.26.201.1 | 80 | 172.25.13.131 | 16.54Kb | 0 | 28.32ms | <1ms | <1ms | <1ms | <1ms |
| 172.26.201.3 | 80 | 172.23.8.6 | 17.66Kb | 0 | 2.02ms | 2.02ms | 63.83ms | <1ms | <1ms |
| 172.26.201.1 | 80 | 172.24.4.26 | 116.50Kb | 0 | 3.21ms | <1ms | <1ms | <1ms | <1ms |
| 172.26.201.99 | 80 | 172.26.3.17 | 14.48Kb | 0 | <1ms | <1ms | <1ms | <1ms | <1ms |

11.3. 应用层会话

每一次应用层会话，XPM 系统都会将其存入本地数据库，存储的内容包括会话 IP（服务端/客户端），端口（服务端/客户端），应用层包头内容（例如，URL，SQL 等），应用层返回码；以及如 9.2.2 内容的 KPI 和 KQI；例如：

| | | | | | | | | | |
|-----------|--------------|----|---------------|-------|-----------------------------|--------|------|-----|-----------|
| 负载均衡前_NAT | 192.168.1.12 | 80 | 192.168.1.108 | 55310 | 192.168.1.12/alertStatistic | 2270 | POST | 200 | <1ms |
| 负载均衡前_NAT | 192.168.1.12 | 80 | 192.168.1.121 | 51889 | 192.168.1.12/ipmDb2Servlet | 563002 | POST | 200 | 2933.34ms |
| 负载均衡前_NAT | 192.168.1.12 | 80 | 192.168.1.121 | 52035 | 192.168.1.12/netStatistic | 1165 | POST | 200 | <1ms |
| 负载均衡前_NAT | 192.168.1.12 | 80 | 192.168.1.108 | 55077 | 192.168.1.12/netStatistic | 1230 | POST | 200 | <1ms |
| 负载均衡前_NAT | 192.168.1.12 | 80 | 192.168.1.108 | 55310 | 192.168.1.12/netStatistic | 974 | POST | 200 | 1.69ms |

11.4. 原始数据包

在 XPM-H 版本，当开启网络流量存储功能后，XPM 会将网络流量以 Raw Packet 格式，存储在本地存储单元；用户可以通过 TCP/UDP 通信对，或应用层会话，或者指定提取的时间和五元组形式进行原始数据包的提取。

11.5. 四种数据格式的关系

- 某个 KPI/KQI 的图形化数据，是多个通信对或应用会话的该 KPI/KQI 的平均值或累计值；
- 告警的阈值都是以图形化数据为参照，而触发的原则是实时值超过了设置的阈值；
- 通过对图形化数据的钻取，可以获得与之对应的通信对或会话；
- 而如果开启流量回溯功能，则可以通过通信对或会话，下载原始数据包（Raw Packet）。

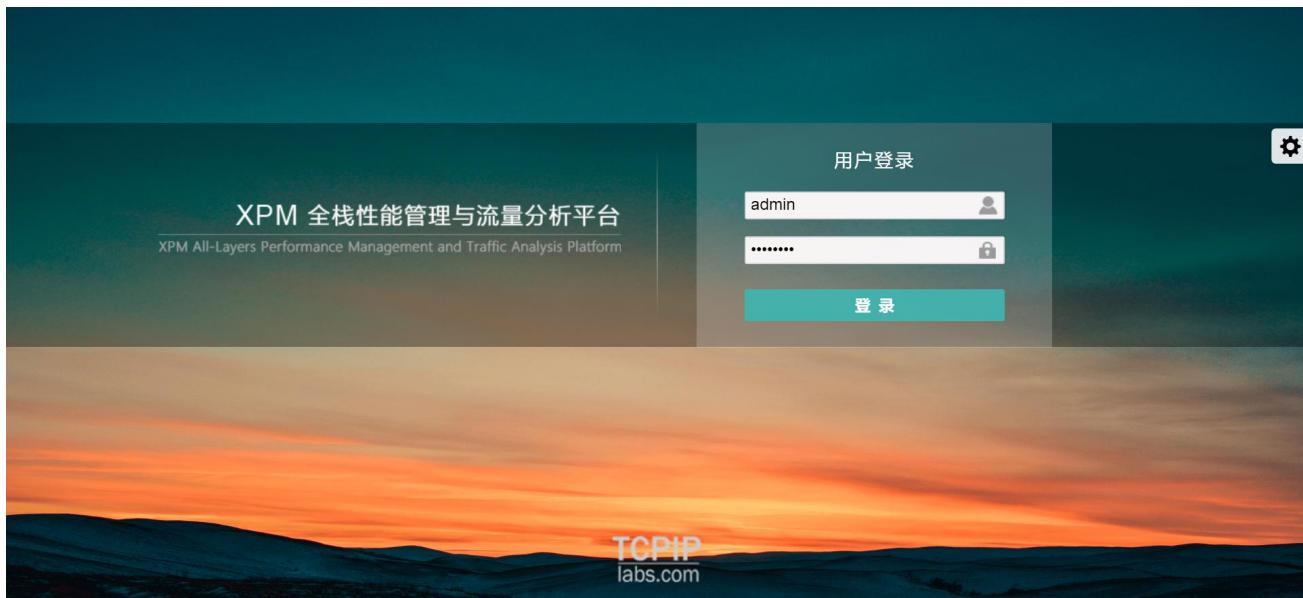
简言之，XPM 的所有功能和使用场景，都是围绕这四种数据而开展，因此，准确的理解这四种数据的逻辑关系和技术关系，对于学习和使用 XPM 都有根本性的意义。

12. 获得使用授权，激活 XPM

12.1. 登录系统

12.1.1. 第一次登陆 XPM

- 通过浏览器访问 XPM 的管理 IP，即可访问和使用 XPM，第一次正常登陆的界面如下截图；
- 如果没有显示如下页面，请检查管理 IP 是否配置正确，或 ping 管理 IP 是否能够连通；
- 如果显示不正常，则需要更换浏览器，浏览器支持情况见下节。



12.1.2. XPM 支持的浏览器种类

- 近 3 年的 Chrome 或 Chrome 内核的浏览器，Firefox 浏览器，Microsoft Edge 浏览器；
- Microsoft 公司的 IE 浏览器我们只支持 IE 10 以上的版本，低于 IE 10 的版本，可能会出现显示或使用异常。

12.1.3. XPM 的默认账号和密码分别是

- 账号：admin
- 密码：ptcs1608

请再登陆后，按照后页的方法尽快修改密码，并添加新的账号。

12.2. 获得使用授权，激活 XPM

- 用户在输入正确的账号和密码后，无论是免费版本还是收费版本，系统都会自动跳转到授权申请和上传页面；
- 用户需要根据该页面的内容，认真填写真实的用户信息，然后，生成一份授权申请文件，并发邮件给 tcpiplabs@outlook.com，以获得授权文件；
- 如果没有授权文件，您将无法使用 XPM。
- 授权申请页面如下：

生成授权信息 -

用户名

联系人

电话

邮箱

最大分析流量 (Mb)

授权模块

| | | |
|--------------------------------|---------------------------------|------------------------------------|
| <input type="checkbox"/> 多观察点 | <input type="checkbox"/> 服务端 | <input type="checkbox"/> 客户端 |
| <input type="checkbox"/> HTTP | <input type="checkbox"/> URL | <input type="checkbox"/> 报文 |
| <input type="checkbox"/> MYSQL | <input type="checkbox"/> ORACLE | <input type="checkbox"/> SQLServer |
| <input type="checkbox"/> 拓扑图 | <input type="checkbox"/> 通信对 | <input type="checkbox"/> 流量储存 |
| | | <input type="checkbox"/> 地图 |
| | | <input type="checkbox"/> iDigger |

确定

上传授权文件 -

上传授权文件

告警信息

12.3. 授权功能页面使用说明

- 最大分析流量：是指用户镜像到 XPM 的最大峰值流量，如果用户不知道该流量的大小，可以预估一个上限；请特别注意，如果超过该上限，XPM 会自动丢弃超过该上限的数据包；
- 对于大部分用户，授权模块的功能都是收费的，因此，请您在勾选该模块之前，向 service@protocolsoft.com 咨询，或 XPM 的线上 IM 沟通，了解每个模块的价格；
- 正确填写本页面的相关内容后，点击【确定】，系统会自动生成一个加密文件，将该加密文件发送给 service@protocolsoft.com，并稍等即可获得授权文件；
- 将新获得的授权文件，在【上传授权文件】功能下，点击【上传授权文件】，即可完成激活 XPM 的流程。

13. 系统设置

13.1. 如何进入系统设置功能

在产品默认首页，在如下图所示的黃圈位置，即可点击进入系统设置功能。



进入后的系统设置主界面如下图所示：



系统设置共有 5 个主要的功能群，从上至下分别是：

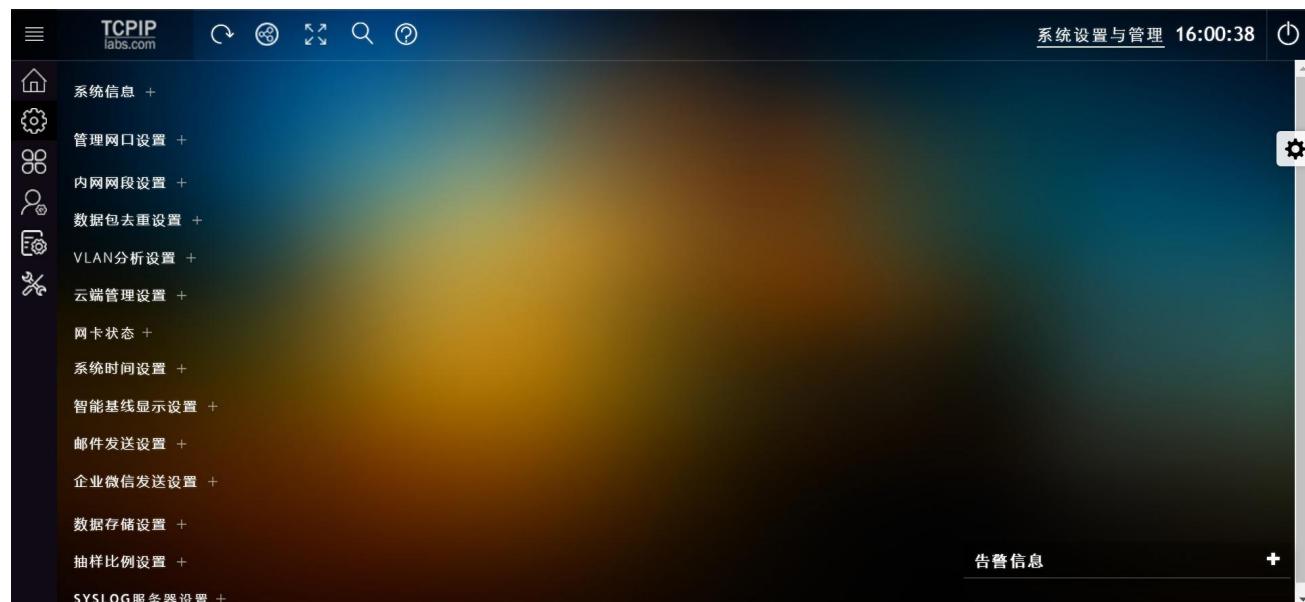
- 系统设置与管理
- 产品更新与授权

- C. 账号管理
- D. 系统日志
- E. 系统工具

现在，就逐一对每个功能群进行详细介绍。

13.2. 系统设置与管理

点击如上图所示，在系统信息旁边的【-】，即可收起系统信息的功能。收起后的系统设置与管理界面如下：

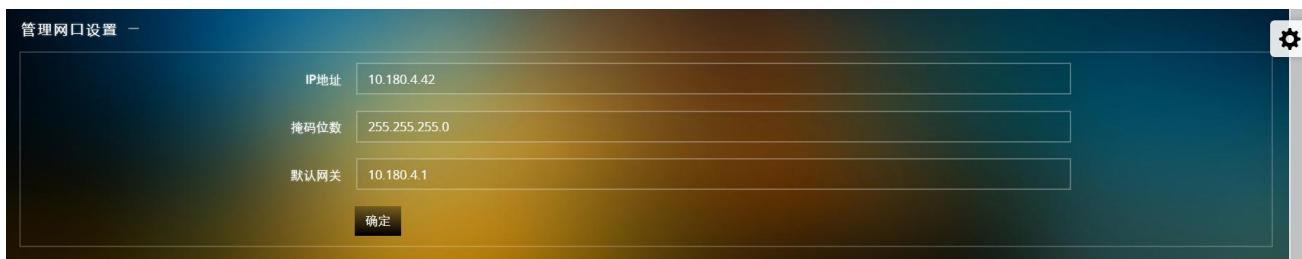


系统设置与管理的每个子功能介绍如下：

13.2.1. 系统信息

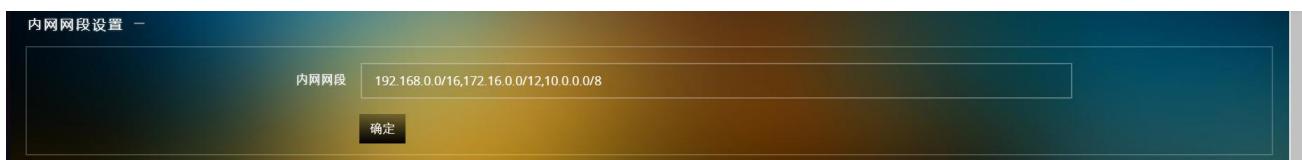
该功能所显示的信息，即为用户申请授权时填写的相关内容，用户需要再次确认，是否与申请的授权信息相一致。该功能不能编辑，不能操作。

13.2.2. 管理网口设置



- XPM 是 B/S 架构的产品，安装 XPM 的硬件或虚拟机，必须配置至少两个网口，一个是工作口（没有 IP），而另一个是管理网口（需要配置 IP），通过该管理网口的 IP，用户可以使用浏览器对 XPM 进行访问和使用；
- 浏览器访问 XPM 的管理 IP 的时候，默认使用的是 HTTP 协议，采用 80 端口；
- 虽然在 XPM 镜像安装过程中，已经设置过管理网口，但如果用户还要改变，则可以在这个位置对管理网口进行调整。

13.2.3. 内网网段设置



- 内网网段，是指位于 XPM 部署位置后端（内测）的服务器区的 IP！
- 输入正确的，完整的服务器区内网网段，是 XPM 输出正确的上下行流量和相关 KPI 的最重要设置！
- 请特别注意：不要把公网的 IP，或者访问服务器区的客户端 IP 设置到这个位置！
- 默认的输入方法为标准的子网输入方法。

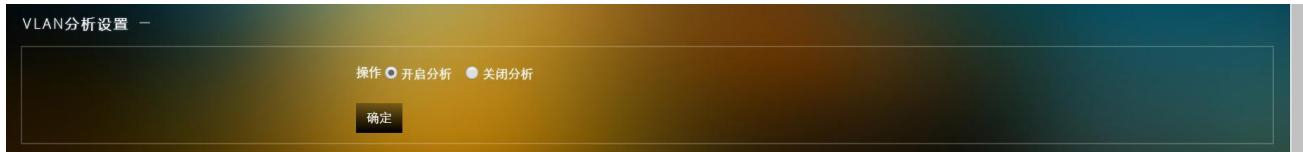
13.2.4. 数据包去重设置



- 默认状态是关闭；
- 该功能用来过滤镜像过程中，可能产生的重复流量；这种情况较为常见，特别是在既要镜像南北向流量，也要镜像东西向流量的时候！

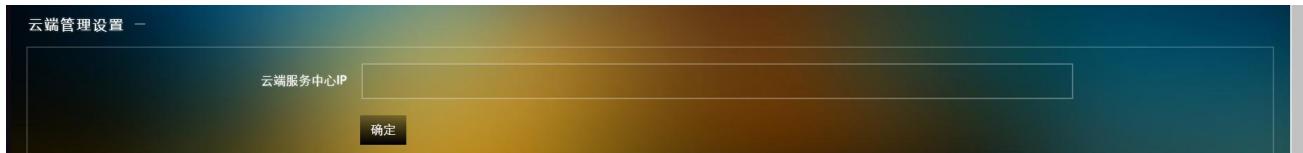
- 系统安装完成后，XPM 的数据包去重功能默认是关闭的，因为此时还需要将 XPM 接收到的流量与 SNMP 网管流量去核对，以确认是否接入正确；
- 请特别注意，一旦确认了接入流量大小与 SNMP 网管一致，就需要立即开启数据包去重功能！否则，很多 KPI 会计算出现错误。

13.2.5. VLAN 分析设置



- 默认状态是开启；
- 该功能用来识别通过流量汇聚设备（TAP）打 VLAN 标签的流量，该 VLAN 标签，通常用来作为标识来自不同交换机的镜像流量；即：如果采用了 TAP 设备为不同镜像流量打 VLAN 标签，则务必要开启此功能；
- 请特别注意：这里的 VLAN 识别，和用于区隔网络访问的 VLAN 不同，但都在 IP 数据包相同的字节位置，只是 bit 位置不同。

13.2.6. 云端管理设置



- XPM 提供云端监控服务，可以帮助用户执行值守和监控工作；该服务是收费服务；
- 用户输入正确的服务中心 IP，即代表用户同意位于云端的 XPM 服务中心，接收用户本地的 XPM 重要的基础指标；
- 本地 XPM 系统只会上传图形化数据，其他类型的数据均不会上传，包括但不限于通信对，应用会话，原始数据包，或其他配置信息；
- 用户可以通过邮件 service@protocolsoft.com，或 XPM 的在线 IM，获取 XPM 云端服务中心的 IP；
- XPM 服务中心的工程师，会在发现用户本地上传的 XPM 监控指标异常时，通过邮件、IM 或其他方法及时与用户联系，以避免产生严重事故。

13.2.7. 网卡状态



The screenshot shows a table titled "网卡管理与设置" (Network Card Management and Configuration) with the following data:

| 网卡名称 | IP地址 | 接收数据包数 | 接收字节数 |
|--------|----------------|---------------|-----------------|
| lo内部通信 | 127.0.0.1 | 69476327795 | 51256197708890 |
| p261p1 | | 9771443 | 1354969512 |
| p261p2 | | 2830059003768 | 911791319699034 |
| em1 | 175.102.15.166 | 101830894 | 16097181045 |
| em2 | | 0 | 0 |

Page: 1 - 5/5

- 该功能没有编辑功能；只能用来显示网卡的相关信息；
- 该功能最大的用途在于，可以帮助用户，在网口较多时，通过判断数据包和字节数，来确认是哪个网口是工作口，哪个是空闲状态；
- 当确认了工作口的网卡名称后，才可以正确的设置观察点功能。

13.2.8. 系统时间设置

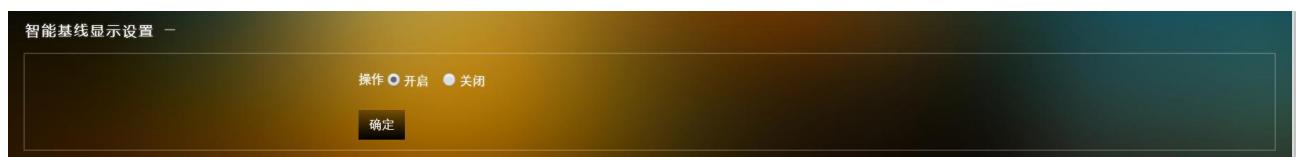


The screenshot shows a form titled "系统时间设置" (System Time Settings) with the following fields:

- 当前系统时间: 2019-08-10 15:45:11
- 时间同步服务器: (empty input field)
- 确定 (Confirm) button

- XPM 的默认系统时间为安装 XPM 的硬件服务器，或虚拟机的时间；
- 如果该时间不准确，还可以在此功能处，自行设置时间同步服务器，设置后，XPM 会以该时间同步服务器的时间，作为 XPM 系统时间；
- 请特别注意：如果用于访问 XPM 的用户个人电脑的时间，与 XPM 服务器的时间有较大差值，会造成数据和显示异常！

13.2.9. 智能基线显示设置



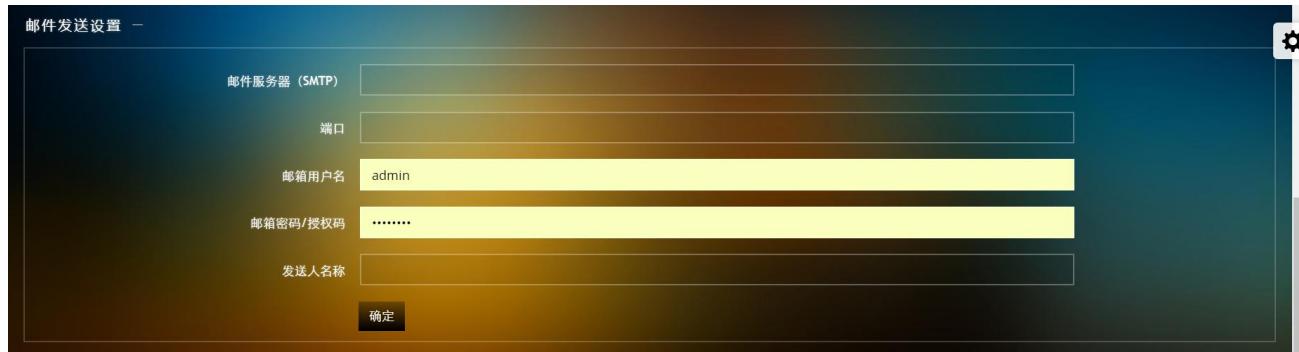
The screenshot shows a form titled "智能基线显示设置" (Intelligent Baseline Display Settings) with the following fields:

- 操作 (Operation): 开启 (Enable) 关闭 (Disable)
- 确定 (Confirm) button

- 该功能是针对告警功能中，开启智能基线告警的 KPI 有效；关于告警功能将在后页详细介绍；
- 该功能默认是关闭状态；开启后，会在已经设置了智能基线告警的 KPI 图形中，看到智能基线出现；
- 但请特别注意：在设置了智能基线功能后，需要在至少 7 天时间后，才能在相关 KPI 图形中，看到该

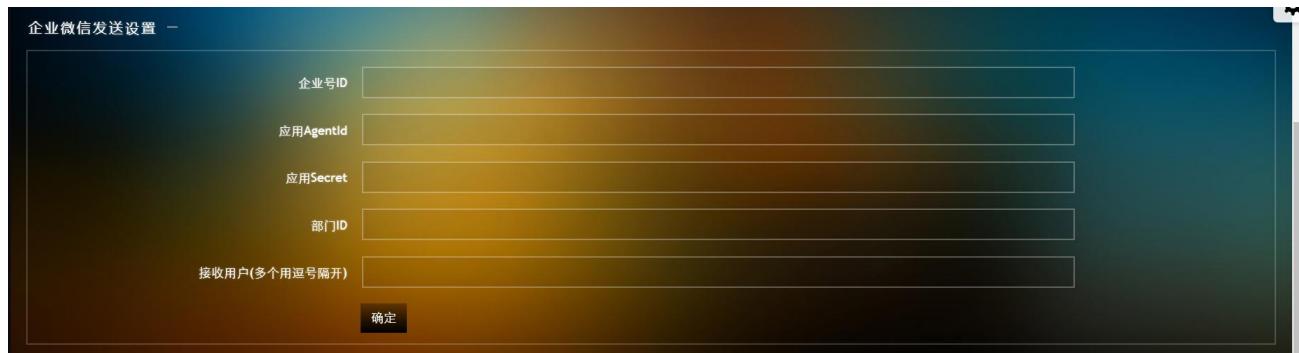
基线出现。

13.2.10. 邮件发送设置



- 此功能用来作为报表发送的发送邮箱用途；
- SMTP 服务邮箱，需要与 XPM 可以通信。

13.2.11. 企业微信发送设置



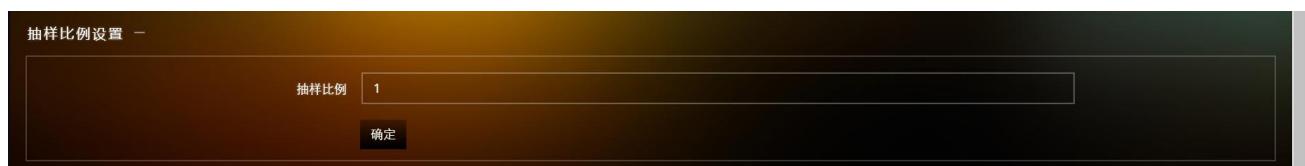
- 对于在内部采用企业微信的单位，用户可以通过配置此功能，将 XPM 的告警信息，通过企业微信发送到相关用户的企业微信客户端。

13.2.12. 数据存储设置



- 该功能主要针对的是流量存储与回溯功能；
- 文件大小是指：存储原始流量的每个文件大小，在流量小于 5Gbps 时，建议使用 500MB；大于 5Gbps 时使用 1GB 的文件大小设置；
- 该功能与 XPM 安装时的磁盘空间划分不矛盾，这里的磁盘利用率是指在系统安装时划分的磁盘空间的基础上的百分比，是对某些特殊情况的一种保护措施；
- 无论是流量存储，本地（存储通信对或应用会话的）数据库，还是图形化数据存储，系统都采用先进先出策略，具体覆盖的周期由用户的实际网络和业务情况决定。

13.2.13. 抽样比例设置



- 当用户的实时网络流量很大，且有可能超过 XPM 服务器的处理能力的时候，可以使用该功能；
- 该功能的默认值为 1，代表不取样；填写数字 2，代表所有网络流量的 TCP/UDP 按照 1/2 取样；填写数字 3，代表 1/3 取样；
- 取样率越高，系统的失真越大，同时，由于取样的原因，相应比例的 TCP/UDP 或应用层会话会丢失；因此，在绝大多数情况下，不推荐开启该功能，而只保留默认的数字“1”，代表不取样。

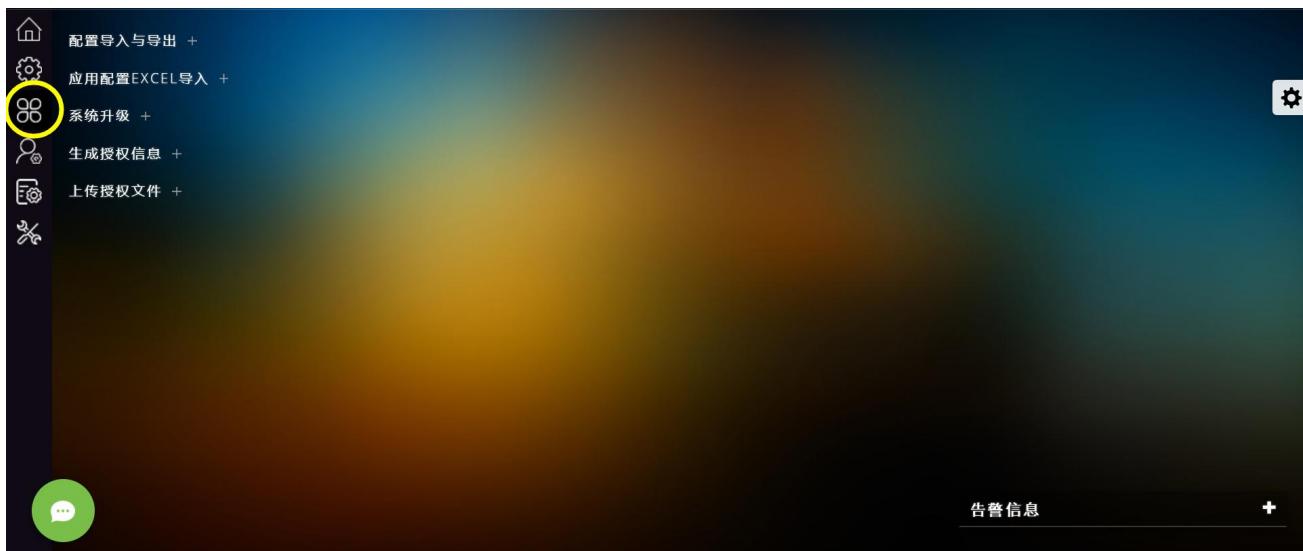
13.2.14. SYSLOG 服务器设置



- 通过正确配置此功能，用户可以把 XPM 的 SYSLOG 和告警信息，通过 SYSLOG 机制发送给其他监控平台，或大数据平台；
- 添加 SYSLOG 接收服务器，请选择列表右上角的【+】，删除为【x】。

13.3. 产品更新与授权

产品更新与授权的主页面如下：

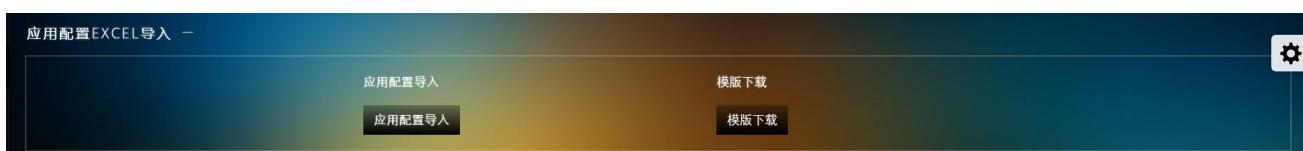


13.3.1. 配置导入与导出



- 该功能用于系统升级，移机，以及其他一些特殊情况；
- 由于用户使用一段时间以后，各种信息都会与设置或配置有关，如果只导出配置，可能会造成很多功能和数据出现异常，因此，除非有 XPM 官方声明的，必须进行配置备份的升级，我们不建议用户自行使用此功能。

13.3.2. 应用配置 EXCEL 导入

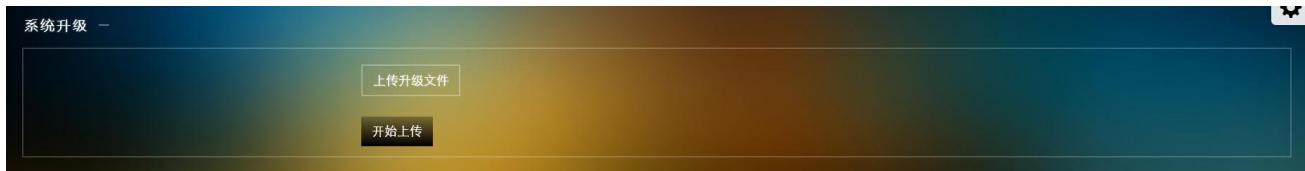


- 此功能主要针对的是 XPM 的服务端和客户端监控功能；
- 当用户需要设置的服务端，客户端很多的时候，可以使用此功能；
- 用户需要先点击【模板下载】，然后，根据下载到本地的 EXCEL 文档的格式和内容，导入需要一次性完

成设置的服务端和客户端信息；

- 填写完成后，再将该 EXCEL 文件点击【应用配置导入】功能，导入到 XPM 系统，即可一次性完成对若干服务端和客户端的设置；
- 当用户需要设置的服务端和客户端，都小于 20 个的时候，不建议使用该功能。

13.3.3. 系统升级



XPM 的系统升级有两种方法：

- 其一，是通过在线升级，XPM 服务中心会自动对可以通信的 XPM 服务器进行远程升级；
- 其二，是通过用户注册的邮箱信息，发送邮件形式，将升级文件发送给用户，用户在本地电脑收到升级文件后，在此功能位置，将升级文件上传到 XPM 服务器。

13.3.4. 生成授权信息，上传授权文件

这两个功能在之前的章节已经介绍，此处不再赘述。

13.4. 账号管理

【账号管理】功能的主界面如下图：

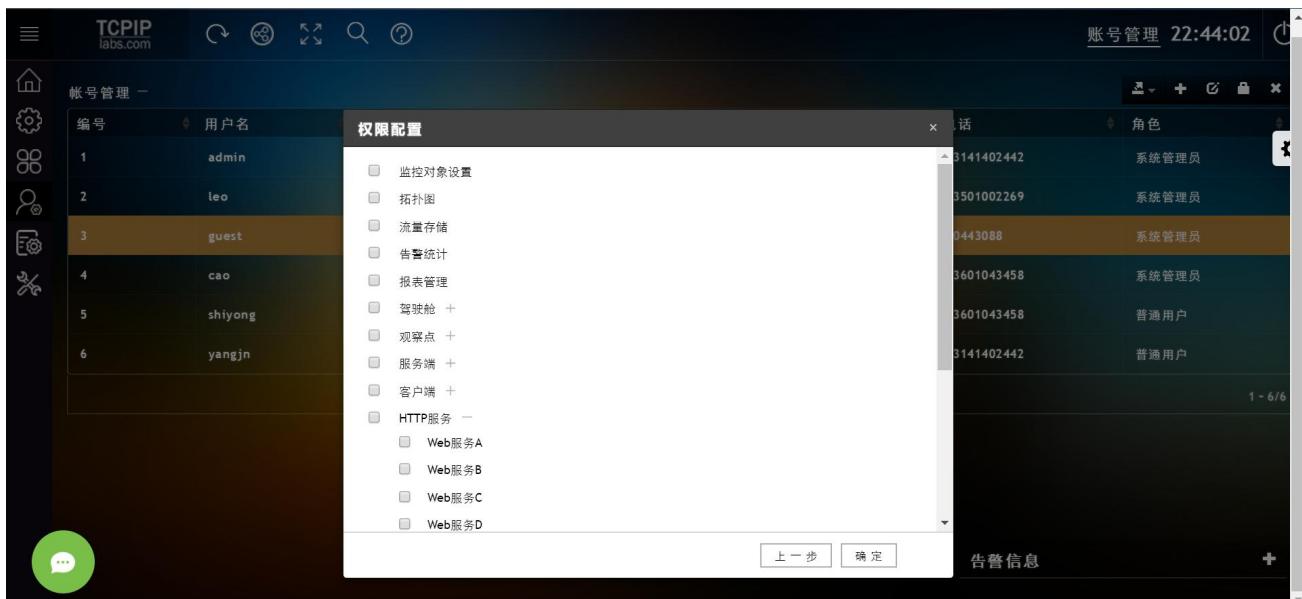
| 编号 | 用户名 | 实际姓名 | 邮箱 | 电话 | 角色 |
|----|---------|-------|------------|------------|-------|
| 1 | admin | info | [REDACTED] | [REDACTED] | 系统管理员 |
| 2 | leo | leo | [REDACTED] | [REDACTED] | 系统管理员 |
| 3 | guest | guest | [REDACTED] | [REDACTED] | 系统管理员 |
| 4 | cao | | [REDACTED] | [REDACTED] | 系统管理员 |
| 5 | shiyong | | [REDACTED] | [REDACTED] | 普通用户 |
| 6 | yangjn | | [REDACTED] | [REDACTED] | 普通用户 |

13.4.1. 添加账号

- 点击列表右上角的【+】，即可弹出如下账号【添加】窗口：



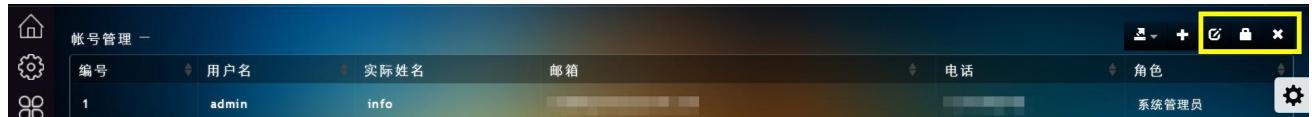
- 根据输入框内容，逐一填写好相关内容即可；
- 请特别注意：当选择最后一项【角色】的【普通用户】选项时，窗口下部的【确定】，会自动改为【下一步】，点击【下一步】，系统会自动跳转到如下窗口内容，管理员用户可根据该窗口内容，对每个普通用户创建不同的使用权限；



- XPM 的账号管理功能非常强大，不仅可以对功能进行使用授权，还可以对每个监控对象进行单独的使用授权；没有授权的监控对象，普通用户无法看到其内容。

13.4.2. 账号管理的编辑，删除和修改密码

- 这三个功能在账号管理列表的右上角，用户根据这三个功能的弹出窗口内容，进行相关操作即可。



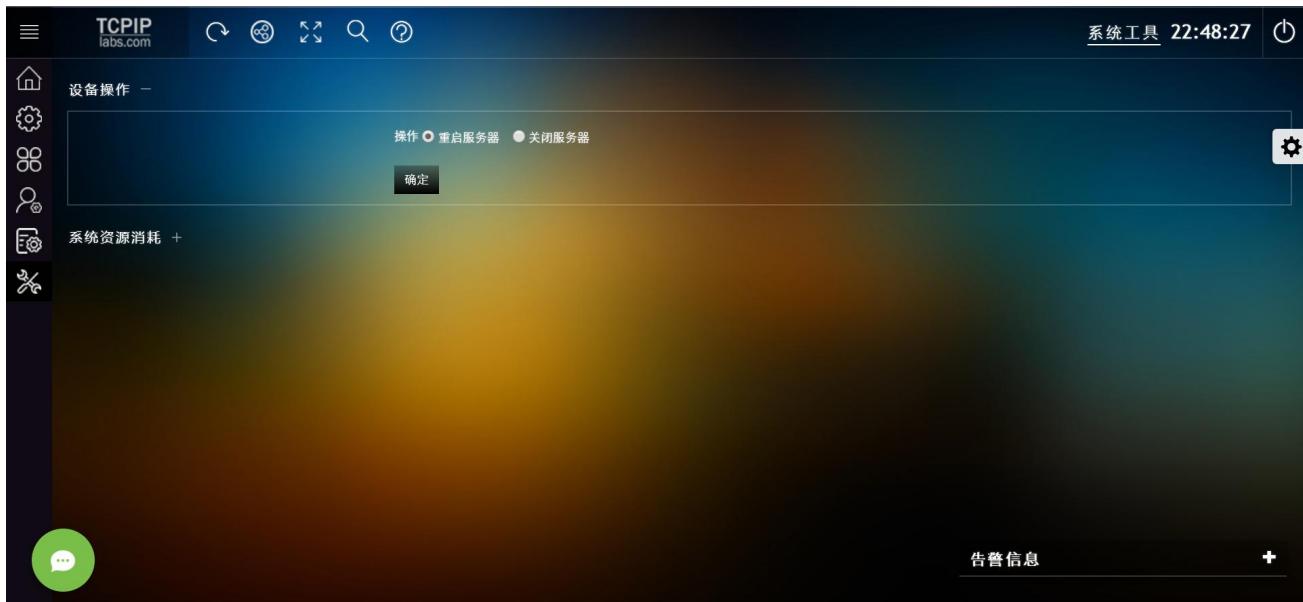
13.5. 系统日志

A screenshot of the XPM system log interface. The top navigation bar includes the XPM logo, a search bar, and a timestamp of 22:42:41. The main area is titled "系统日志" and shows a table of log entries. The columns are 编号 (ID), 时间 (Time), 用户 (User), 模块 (Module), and 信息 (Information). The information column contains log messages such as "应用配置导出" (Application configuration export), "admin用户登录" (admin user login), and "admin用户登录超时, 强制退出" (admin user login timeout, forced logout). On the far left of the log table, there are several small circular icons representing different log types. One specific icon, which looks like a gear or wrench, is circled in yellow. In the top right corner of the log table, there is a small export icon (a sheet of paper with a double arrow) also highlighted with a yellow box.

- XPM 会记录下每位用户对 XPM 的主要登陆、创建、修改、删除等行为的操作；
- 被记录下的这些操作，用户无法编辑或删除；
- 如果需要导出这些系统日志，可以选择列表右上角的【导出数据】功能，并可以选择导出的文件格式。

13.6. 系统工具

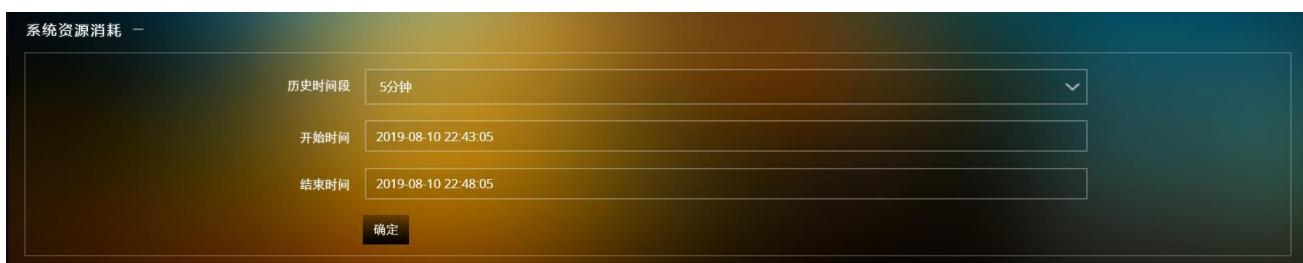
系统工具是 XPM 进行自身监控的重要功能，在大多数情况，用户并不需要使用该功能。系统工具的主界面如下图所示：



13.6.1. 设备操作



13.6.2. 系统资源消耗



- 选择时间段，和开始、结束时间后，**XPM** 会单独开启一个网页，如下图，用户可以通过该网页查看 XPM 各个程序对 CPU、内存的使用情况；
- 用户可以通过页面下部的【+】，对该页面所呈现的内容进行调整；
- 如果使用 XPM 的过程中，长期出现系统反应缓慢的情况，建议使用此功能，查看【系统负载】是否长时间超高。如果系统负载 (payload) 数值长时间高于 70%，则代表系统始终处在较为繁忙的处理状态，我们建议在这种情况下，应尽快增加系统的硬件配置，例如 CPU，内存，或调整磁盘阵列的性能；



14. 监控对象设置

14.1. 监控对象种类

| 序号 | 监控对象 | 适用范围 |
|----|--------------|---|
| 1 | 观察点 | 适用于监控网络链路，运营商专线，网络串行设备 |
| 2 | 服务端 | 对外提供服务的一个或一组 IP，或 NAT 设备；分析粒度为 TCP/UDP 连接 |
| 3 | 客户端 | 客户端，子网，分支机构；分析粒度为 TCP/UDP 连接 |
| 4 | HTTP 服务 | 采用 HTTP 协议的网络服务；Web，中间件等；分析粒度是 HTTP 会话 |
| 5 | Oracle 服务 | Oracle 数据库；分析粒度是 Oracle SQL 语句 |
| 6 | MySQL 服务 | MySQL 数据库；分析粒度是 MySQL SQL 语句 |
| 7 | SQLserver 服务 | SQLserver 数据库；分析粒度是 SQLserver SQL 语句 |
| 8 | URL 服务 | 采用 URL 进行业务定义的网络服务；分析粒度是 HTTP 会话 |
| 9 | 报文交易 | 采用 JSON，XML，HTML 进行业务定义的服务；分析粒度是 HTTP 会话 |
| 10 | 应用可用性 | 对外提供服务的 IP:Port；拨测形式，只监控存活状态 |

14.2. 进入监控对象设置

默认首页，左侧主要功能栏，第二个功能即为【监控对象设置】



点击进入后，即为下图：

| 观察点名称 | 网卡名 | VLAN ID | 上行带宽 [Mb] | 下行带宽 [Mb] |
|-------|------|---------|-----------|-----------|
| | lo | 444 | 100 | 100 |
| | lo | 555 | 100 | 100 |
| | lo | 666 | 100 | 100 |
| | lo | 777 | 100 | 100 |
| | eth0 | 0 | 100 | 100 |

14.3. 观察点管理与设置

- 观察点，是指交换机的流量镜像点，同时也支持 VXLAN，MPLS 这类隧道协议作为一种镜像流量，通常观察点不止一个；
- 观察点通常被用来作为监控网络链路，串行的网络设备，运营商专线。

| 观察点名称 | 网卡名 | VLAN ID | 上行带宽 [Mb] | 下行带宽 [Mb] |
|-----------|------|---------|-----------|-----------|
| 负载均衡前_NAT | lo | 444 | 100 | 100 |
| 负载均衡后_NAT | lo | 555 | 100 | 100 |
| 防火墙前 | lo | 666 | 100 | 100 |
| 防火墙后 | lo | 777 | 100 | 100 |
| XPM演示DEMO | eth0 | 0 | 100 | 100 |

14.3.1. 新增，编辑，删除观察点

在观察点列表的右上角，功能依此为：列选择，导出数据，告警设置，新增，修改，删除；这些功能通过弹出窗口提示即可完成。需要注意的要点包括：

- XPM 支持将多个网口（VXLAN/MPLS）聚合为一个观察点；
- 上下行带宽必须设置，该设置与带宽利用率有关；对于全双工以太网，都是双向相同速率。

新增

| | |
|-------------|--------------------------|
| 名称 | <input type="text"/> |
| 网卡名 | <input type="text"/> 请选择 |
| VLAN ID | <input type="text"/> 请选择 |
| VXLAN ID | <input type="text"/> 请选择 |
| MPLS LABEL1 | <input type="text"/> 请选择 |
| MPLS LABEL2 | <input type="text"/> 请选择 |
| MPLS LABEL3 | <input type="text"/> 请选择 |
| MPLS LABEL4 | <input type="text"/> 请选择 |
| MPLS LABEL5 | <input type="text"/> 请选择 |
| 上行带宽[Mb] | <input type="text"/> |
| 下行带宽[Mb] | <input type="text"/> |
| 重新开始分析 | <input type="checkbox"/> |

1. 如果有多个监控对象要设置，可以在最后一个设置完后再选择重启分析程序。
 2. 添加观察点涉及多个网卡，需在添加完最后一个观察点后手动重启物理机器。
 (系统设置-系统工具-设备操作)

14.4. 服务端管理与设置

服务端管理与设置 -

| 服务端名称 | 服务端IP端口 | 带宽[Mb] | 备注 |
|-------|-------------------|--------|----|
| 业务系统A | 192.168.1.11 | 100 | |
| 业务系统B | 192.168.5.51:7001 | 100 | |
| 业务系统C | 10.111.15.1:40073 | 100 | |
| 业务系统D | 10.111.7.3:56277 | 100 | |

在服务端列表的右上角，功能依此为：列选择，导出数据，告警设置，新增，修改，删除；这些功能通过弹出窗口提示即可完成。需要注意的要点包括：

- 服务端输入的表达形式，请务必按照弹出窗口的提示严格匹配；
- 新增、修改或删除服务端设置时，相关分析程序需要重启，因此，可能会在图形上出现断点情况；



14.5. 客户端管理与设置

内容与服务端相似，请参考上一节“服务端设置与管理”。

14.6. HTTP 服务管理与设置

HTTP 服务管理与设置，主要内容与服务端相似，请参考上一节“服务端设置与管理”。但有两个要点要特别注意：

14.6.1. 解析、存储 HTTP 负载段报文内容，并检索关键词

- 在 HTTP 服务列表右上角的快捷功能栏的第 4 个功能【开启负载入库】，是 HTTP 特有功能；



- 该功能可以对负载段的 JSON, XML, HTML 内容进行解析，并写入本地数据库；
- 这一功能的主要应用场景适用于对各类业务数据进行查询和审计，例如，表单。
- 查询功能的位置在产品页面最上面的快捷工具栏，第 4 个功能【搜索查询】，如下图：



点击该【搜索查询】功能，会弹出如下窗口：



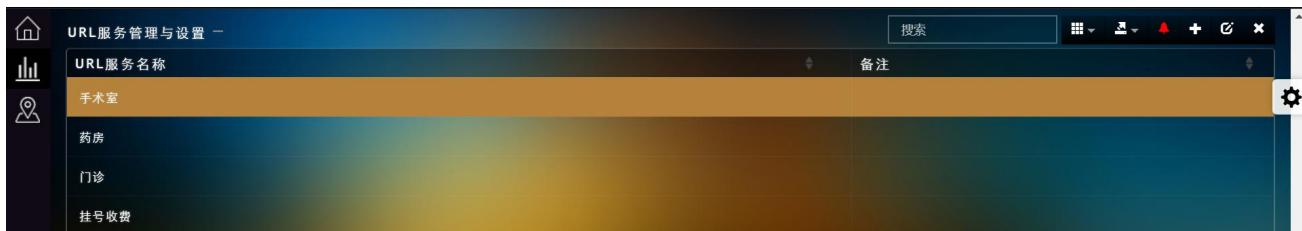
逐一选择 XPM 服务器，时间，并在【报文】输入框中输入需要查询的负载段的特征文本，XPM 就可以输出该文本的内容和对应的 HTTP 会话。

14.7. Oracle/MySQL/SQLserver 服务管理与设置

除了监控对象的 IP 和 Port 的表达形式与服务端不同外，这 3 个数据库监控对象的新增，修改，删除等功能与服务端基本相同，具体请参考服务端管理与设置章节。

14.8. URL 服务管理与设置

- URL 交易监控，是 XPM 的特色功能之一，也是非常实用的业务级监控功能！
- 我们知道，绝大多数的 B/S 架构的业务，前端的页面都包含有很多的 URL，这些 URL 中，只有一部分执行了具体的业务操作，其余的诸如静态图片 URL，样式 URL 等，并不属于业务级交互；显然，将所有 URL 都监控，并以此为依据输出相关指标显然是不准确的，甚至是错误的。因此，对承载业务交互内容的 URL 进行独立的监控和分析，才是符合业务需求的功能理解。XPM 的 URL 服务性能监控即是专门为此应用场景所设计的功能群组。



14.8.1. 如何监控一个多操作步骤的 URL 业务？

URL 交易，都是由若干次操作组成，每次操作都是一个与后端进行交互的 URL，因此，将这些 URL 组合在一个监控对象，即可完成对此业务的监控和分析。点击 URL 服务管理与设置列表的右上角新增功能【+】，或

修改【】，即可弹出如下窗口：



根据窗口内的功能提示，即可完成对一个由多个 URL 组成的业务的新增或修改。

14.9. 应用可用性管理与设置

应用可用性管理，是采用拨测方法，对服务端进行端口探测，以确认该服务是否正常或宕机，此功能在基础监控中也经常被采用。

| 应用可用性管理与设置 - | | | | | |
|--------------|---------------|------|---------|---------------------|----|
| 名称 | IP | 端口 | 间隔时间[分] | 上一次执行时间 | 状态 |
| TEST01 | 192.168.5.51 | 7001 | 5 | 2019-08-11 14:51:00 | 开启 |
| TEST03 | 192.168.1.250 | 8080 | 30 | 2019-08-11 14:50:00 | 开启 |

点击应用可用性管理与设置列表的右上角新增功能【+】，或修改【】，即可弹出如下窗口：

用户根据此弹出窗口的提示完成每一项设置即可。

15. 告警相关功能

15.1. 必须了解的告警算法要点

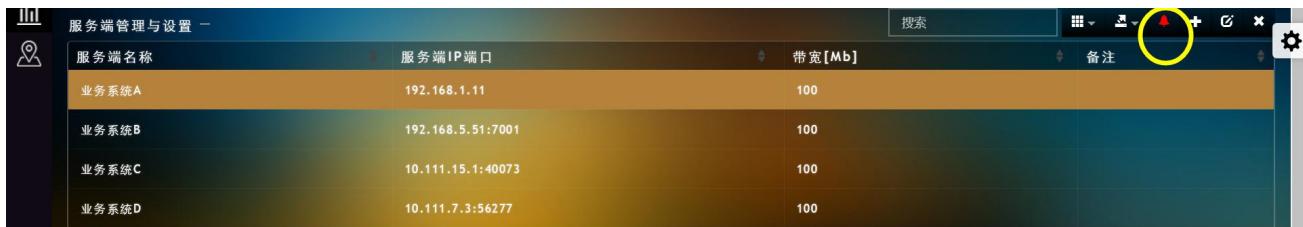
关于 XPM 的告警算法，有如下要点需要特别说明：

- XPM 对所有监控对象的告警方法，都分为人工阈值和智能告警两种；
- 两种告警算法，都是以监控对象某个指标的平均值为触发条件，该平均值即为当前时段，所有 TCP/UDP 或应用会话的该指标的平均值；
- 对于性能指标，我们建议采用人工阈值；对于状态指标，建议采用智能告警算法；
- 人工阈值和智能告警，都可以对高阈值和低阈值进行设置并发出告警；
- 人工阈值有三个级别，分别是普通，重要，紧急；
- 智能告警只有一个级别，该告警级别是按照当前 KPI 数值超过基线的百分比而确定；
- XPM 采用了更为合理的基线算法，有效避免了多次极值对基线的偏离影响；
- 为了降低虚警和误警比率，XPM 采用了合理的告警抑制算法，可以有效规避偶尔发生的短暂的波峰或波谷对告警的影响。

15.2. 告警阈值设置

15.2.1. 告警阈值设置的功能入口

- 对所有监控对象的告警设置，均在左侧工具栏的第二个主要功能【监控对象设置】中完成；具体的功能位置在每个监控对象列表的右上角，以【】为示意，即为告警设置；如下图：



- 点击告警设置功能【】后，页面会自动下移到该监控对象的 KPI/KQI 列表，如下图：

| 服务端告警设置 | | | | | | | | |
|-------------|---------|---------|---------|---------|---------|---------|---------|---------|
| KPI名称 | 普通告警[低] | 重要告警[低] | 紧急告警[低] | 智能告警[低] | 普通告警[高] | 重要告警[高] | 紧急告警[高] | 智能告警[高] |
| 访问质量[ms] | - | - | - | - | - | - | - | - |
| 负载传输时延[ms] | - | - | - | - | - | - | - | - |
| 服务端通信时延[ms] | - | - | - | - | - | - | - | - |
| 客户端通信时延[ms] | - | - | - | - | - | - | - | - |
| 链路时延RTT[ms] | - | - | - | - | - | - | - | - |

- 用鼠标选中需要设置的 KPI/KQI，再点击该列表右上角的修改功能【】，即会弹出该 KPI/KQI 的告警设置窗口，如下图：



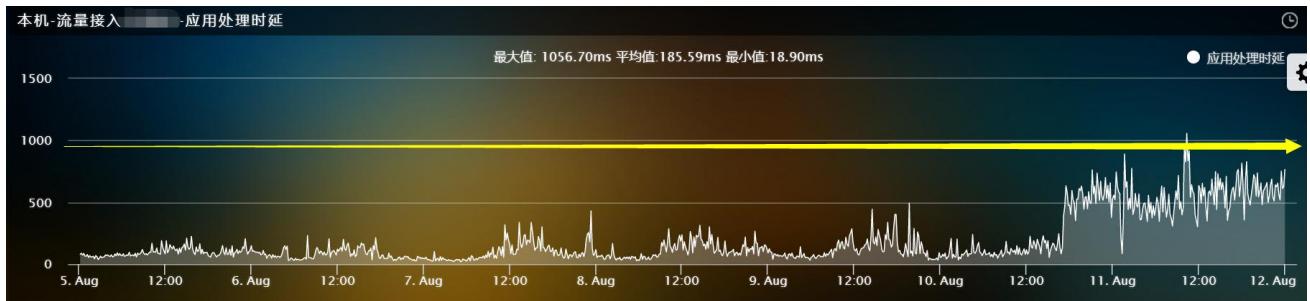
此窗口的设置非常重要，请务必理解如下内容：

- 1) 普通告警, 重要通告警, 紧急通告警, 都是对人工阈值算法有效;
- 2) 左侧四个输入框, 是对低阈值有效; 右侧四个输入框, 对高阈值有效;
- 3) 输入阈值数值后, 是否开启对该 KPI/KQI 的告警功能, 要以是否勾选【阈值开启】后面的低阈值和高阈值的选择框 为准;
- 4) 对于性能指标, 我们建议采用人工阈值; 对于状态指标, 建议采用智能告警算法;
- 5) 智能告警设置后, 需要至少运行 7 天后, 才能生效;
- 6) 如果有多个类型相同的监控对象需要设置相同的 KPI/KQI 阈值, 可以勾选【全局设置】, 以降低设置重复性和工作量。

15.2.2. 如何合理的设置性能指标 KQI 的告警阈值

如前所述, 我们强烈建议, 对 KQI (时间类指标, 错误类, 未响应类指标) 采用人工阈值, 因为这些指标与业务质量和用户感知之间相关, 有一个相对合理的, 固定的范围。那么, 如何确定 KQI 的合理阈值范围呢?

我们建议，如果监控那个对象在过往几天，没有发生事故或投诉，则可以这几天时间的峰值或谷值，作为人工阈值中，普通告警的高阈值和低阈值，重要告警则再向上浮动 50%，紧急告警浮动 100%；例如：



对于该图例，我们建议的普通告警阈值为 1000ms；重要告警阈值为 1500ms；紧急告警阈值为 2000ms。

15.2.3. 如何合理的设置状态指标 KPI 的告警阈值

由于状态指标 KPI 没有绝对的合理范围，例如，网络流量，会话量，包速率等，但突变代表了一种风险或异常，因此，采用智能告警算法更为合适。

而对于大部分没有稳定运行规律的业务或网络环境，为了降低虚警和误警概率，我们建议智能告警的阈值不低于 100%。即：当某个 KPI 的当前值与过往 7 天的基线值相比，超过了 100% 的变化量时，即发出告警。

15.3. 告警信息获取和钻取

15.3.1. 告警信息的获取

XPM 的告警提示共有三个地方，分别是：告警信息浮动窗，默认驾驶舱的告警柱状图，业务链驾驶舱小列表的健康度。

- 【告警信息】浮动窗，在页面的右下部；如下图，点击浮动窗右侧的【+】，即可展开告警内容；



- 默认驾驶舱的告警柱状图



- 业务链驾驶舱小列表的健康度



15.3.2. 告警信息的钻取

- 单击【告警信息】→跳转到【告警图形】→拖拽告警图形的波峰或波谷→获得导致告警发生的【通信对或会话】。

| 发起时间 | 服务端IP | 客户端IP | 网络流量 | 连接发起数量 | 链路时延RTT |
|----------------|--------------|----------------|----------|--------|----------|
| 08-12 00:51:20 | 172.17.0.102 | 117.136.41.127 | 370.53Kb | 0 | 970.28ms |
| 08-12 00:51:20 | 172.17.0.101 | 117.191.29.160 | 2.12Mb | 12 | 38.53ms |
| 08-12 00:51:20 | 172.17.0.101 | 223.9.44.235 | 4.52Mb | 12 | 21.64ms |
| 08-12 00:51:20 | 172.17.0.102 | 106.35.24.240 | 16.89Kb | 2 | 20.63ms |
| 08-12 00:51:20 | 172.17.0.102 | 223.9.44.235 | 2.18Mb | 16 | 20.57ms |
| 08-12 00:51:20 | 172.17.0.101 | 117.136.41.127 | 1.37Mb | 0 | 16.80ms |
| 08-12 00:51:20 | 172.17.0.102 | 1.70.45.192 | 268.82Kb | 8 | 14.17ms |
| 08-12 00:51:20 | 172.17.0.102 | 61.148.243.94 | 26.06Kb | 4 | 12.59ms |
| 08-12 00:51:20 | 172.17.0.101 | 1.70.45.192 | 1.43Mb | 4 | 10.32ms |

- 如果是 XPM-H 版本，并且开启了流量存储和回溯功能，再次点击如上截图中的任意一条通信对信息，页面会自动下移到 10s 钟粒度的通信对信息列表，如下图：

| 详细列表 | | | | | | 搜索 | 导出 | 打印 | 刷新 |
|----------------|--------------|----------------|--------|--------|---------|----|----|----|----|
| 发起时间 | 服务端IP | 客户端IP | 网络流量 | 连接发起数量 | 链路时延RTT | | | | |
| 08-12 00:51:20 | 172.17.0.101 | 117.191.29.160 | 2.12Mb | 12 | 38.53ms | | | | |

- 再次点击该列表右上角的下载功能【】，根据提示，可以将该通信的原始流量，以 PCAP 文件格式下载到本地，用户可以用 Wireshark 等数据包解析工具打开并做进一步分析。

15.4. 告警统计分析功能

15.4.1. 告警统计分析功能的入口

在左侧主要功能栏的第 5 个功能，和告警信息浮动窗左下角，都有该功能的入口。如下图黄圈中所示：



点击进入后，告警统计功能的页面如下图所示：



15.4.2. 告警信息的字段

告警信息的字段包括但不限于：时间，监控对象，告警级别，告警类型，响应状态，响应人，响应时间，可能原因，联系人，电话，email；

15.4.3. 告警统计分析的维度

XPM 的告警统计分析功能异常强大，可以按照如下维度，对各个告警信息进行详细的统计分析。

- 时间维度
- 监控对象维度
- KPI/KQI 维度
- 告警级别维度
- 相应状态维度

统计分析后的每一条告警信息，也都可以通过双击，钻取到通信对或应用会话（如果还没有被新数据所覆盖）。

15.4.4. 告警信息的导出

统计分析后，如果需要输出统计分析的告警信息，可以在告警信息列表右上角第 2 个功能【导出数据】选择文件格式后导出。



| 开始时间 | 结束时间 | 用户名 | 告警来源 | 模块名称 | 业务名称 | KPI名称 | 告警类型 | 告警级别 | 响应状态 | 响应 | 操作 |
|---------------------|---------------------|-----|-----------|--------|--------|-----------|------|------|------|----|----|
| 2019-08-12 01:14:00 | 2019-08-12 01:15:00 | 本机 | 负载均衡前_NAT | URL服务 | 护理 | Web服务响应时延 | 高阈值 | 普通 | 未响应 | - | |
| 2019-08-12 01:14:00 | 2019-08-12 01:15:00 | 本机 | 负载均衡后_NAT | URL服务 | 护理 | Web服务响应时延 | 高阈值 | 普通 | 未响应 | - | |
| 2019-08-12 01:12:20 | 2019-08-12 01:17:20 | 本机 | 防火墙前 | HTTP服务 | Web服务A | 链路时延RTT | 高阈值 | 紧急 | 未响应 | - | |
| 2019-08-12 01:12:10 | 2019-08-12 01:17:10 | 本机 | 负载均衡前_NAT | 服务端 | 业务系统A | 网络丢包率 | 高阈值 | 普通 | 未响应 | - | |
| 2019-08-12 01:12:10 | 2019-08-12 01:17:10 | 本机 | 负载均衡后_NAT | 服务端 | 业务系统A | 网络丢包率 | 高阈值 | 普通 | 未响应 | - | |
| 2019-08-12 01:12:10 | 2019-08-12 01:17:10 | 本机 | 防火墙前 | 服务端 | 业务系统A | 网络丢包率 | 高阈值 | 普通 | 未响应 | - | |
| 2019-08-12 01:12:10 | 2019-08-12 01:17:10 | 本机 | 防火墙后 | 服务端 | 业务系统A | 网络丢包率 | 高阈值 | 普通 | 未响应 | - | |

16. 页面基础操作



16.1. 快捷工具栏

上图中的蓝色方框内功能。

从左至右，分别是时间回溯，实时刷新，拓扑查询，驾驶舱锁定，全屏，搜索查询，帮助。

16.1.1. 时间回溯

该功能可以对当前页面下，所有的图形，数字，进行全量的时间回溯统计。不同回溯时间段，对应不同的时间粒度，以当前时间为基准，回溯时间段与粒度的对应关系为：

- A. 回溯 4h，粒度为 10s
- B. 回溯 1d，粒度为 1m
- C. 回溯 1w，粒度为 10m
- D. 回溯 1y，粒度为 1h

如上时间粒度是经过充分的调研和实践而得出，但在某些时候，在回溯时间段较长，而回溯粒度较大时，可能会出现回溯出来的数据，与实际感受不同的情况，但这是一种正常情况，原因是由于时间粒度较大所致。

16.1.2. 刷新

该功能主要针对的是当前页面的刷新操作，不是实时计算的频率。共有四个选择。从左至右分别是：立即刷新，10s，30s，60s。每个选择都代表了当前页面每次更新数据的频率。

请特别注意：刷新功能只是浏览器功能，不是后台数据计算频率；XPM 的实时计算和输出频率为 10s，为企业同类型产品最快；

16.1.3. 拓扑查询

该功能是 XPM 重点功能之一，是【拓扑图】功能的一部分，在后页会详细介绍。

16.1.4. 锁定/解锁

该功能用来对当前已经设置完成的驾驶舱，进行锁定，锁定后就不能再进行编辑，适用于多个用户使用同一个驾驶舱的情况。

16.1.5. 全屏

点击该功能，用户浏览器会进入【全屏】模式，退出时按 ESC，该功能生效时会隐藏掉与显示内容无关的浏览器其他功能，适用于监控大屏使用。

16.1.6. 搜索查询

该功能是用户使用 XPM 过程中，最常用的通用功能之一。搜索查询功能，可以对所有监控对象的入库信息进行查询并输出，适用于用户排障，或处理客户投诉。

- A. TCP/UDP 通信对。查询条件为服务端 IP，或客户端 IP；
- B. HTTP/URL 服务。查询条件为 URL 或 URL 里的关键字；
- C. Oracle/MySQL/SQLserver。查询条件为 SQL 或 SQL 里的关键字；
- D. 对于开启了 HTTP 负载入库，或报文交易监控的用户，可以通过搜索负载段的关键字进行查询。

16.1.7. 帮助

对于部分主要页面，会提示页面的操作帮助，我们强烈建议用户应该熟练掌握这些常用页面的基础操作。

在该功能弹出窗口的最下面，也有本《用户手册》的链接。

16.2. 主要功能栏

上图中黄色方框内。

从上至下分别是：首页，监控对象设置，拓扑图，流量存储，告警统计，报表管理，系统设置。

- 首页。系统的默认首页是监控对象驾驶舱；
- 监控对象设置。已经在前页介绍，请参见相关内容；
- 拓扑图。将在后页独立章节介绍；
- 流量存储。将在后页独立章节介绍，该功能只对 XPM-H 有效；XPM-S 和 XPM-V 不会加载该功能；
- 告警统计。已经在前页介绍，请参见相关内容；
- 报表管理。将在后页独立章节介绍；
- 系统设置。已经在前页介绍，请参见相关内容。

16.3. 线上 IM 帮助

在页面左下角紫色圆圈内。

该功能只对 XPM 中文版，且只有购买了线上服务的用户有效，对英文版本无效。

在 XPM 可以与互联网通信的前提下，点击该功能，可以出现如下图所示，用户可以与 XPM 的线上专家进行在线沟通，高效率的帮助用户解决一些产品使用和应用场景的问题。



16.4. 告警信息浮动窗

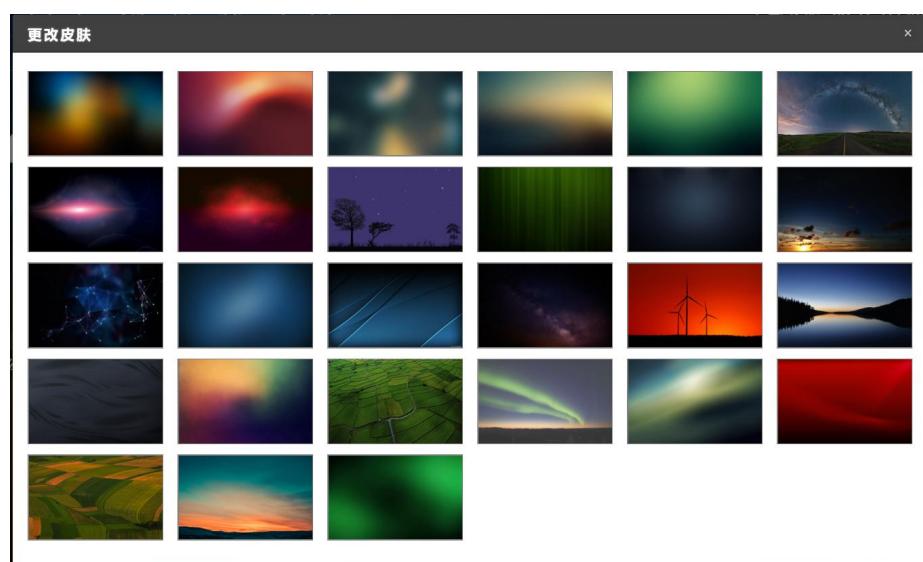
在页面右下角绿色圆圈内。告警浮动窗的相关内容已在前页介绍，请查看相关章节。

16.5. 皮肤设置

在页面右侧上部，滚动条旁边，红色圆圈内。

XPM 的 Web 页面采用半透明设计风格，因此，页面背景也可以通过皮肤设置功能进行更换，非常美观华丽。

默认加载的背景如下图所示：



17. 三种驾驶舱的功能与操作

XPM 具备优秀的易用性，以用户日常监控用途的驾驶舱为例，XPM 提供了三种，分别适应三种应用场景：

| 驾驶舱名称 | 用途与应用场景 |
|---------|---|
| 监控对象驾驶舱 | 系统登陆后的默认首页，可以对每个监控对象进行全面的监控； |
| 统计分析驾驶舱 | 可以对某一类监控类型的所有监控对象，进行横向的统计分析和对比； |
| 业务链驾驶舱 | 完全自定义的驾驶舱，可以用来对不同类型监控对象进行纵向的业务链形态的监控；可以作为监控大屏的上屏界面； |

17.1. 监控对象驾驶舱

系统登陆后的默认首页；每名用户登陆后，系统会记录下其默认首页的内容，并在下次登陆时呈现。



- 通过对图中黄色方框的下拉菜单的选择，可以改变驾驶舱的监控对象；
- 右上角的四个数字所对应的监控指标 KPI/KQI，和右侧的告警柱状图不能更改；
- 其他的图形，可以通过最后面的【+】，进行添加和修改；
- 通过页面上部的快捷工具栏的【时间回溯】功能，可以回溯驾驶舱的所有数据和图形；
- 页面上所有的数字，图形（包括柱状图，线图，饼图等），均可以钻取到 TCP/UDP 通信对或应用会话。



17.2. 统计分析驾驶舱

统计分析驾驶舱，可以用来对相同类型的不同监控对象，进行横向对比，特别是与快捷工具栏的【时间回溯】功能相结合时，可以快速发现哪些服务的质量是最不好的，哪些是最活跃的。



- 点击该列表的列名，可以对该列的 KPI/KQI 数值进行排序；
- 在第一列，选择任意一个监控对象，列表下面的图形也会改变为该监控对象的内容；
- 列表里所有的数字，以及下面的图形，都可以进一步钻取到 TCP/UDP 通信对或应用会话；
- 列表的内容，可以通过列表右上角的【数据导出】功能，导出为特定格式文件。

17.3. 业务链驾驶舱

业务链驾驶舱是 XPM 用户日常监控的重要工具，其功能非常强大；主要体现在：

- 完全的画板式驾驶舱，用户可以自定搭建，改变其中的内容；
- 还有文字，联系，圆角框，图标示例等辅助标注和美化功能；
- 一个 XPM 系统，可以创建多个业务链驾驶舱，并且赋予权限给不同用户；
- 业务链驾驶舱特有监控对象小列表，和健康度功能；非常适合投屏显示；
- 驾驶舱内部，可以添加小列表，也可以添加图形等元素；
- 添加到驾驶舱的数字、图形，均可实现完整的钻取功能。

17.3.1. 如何创建一个新的业务链驾驶舱？

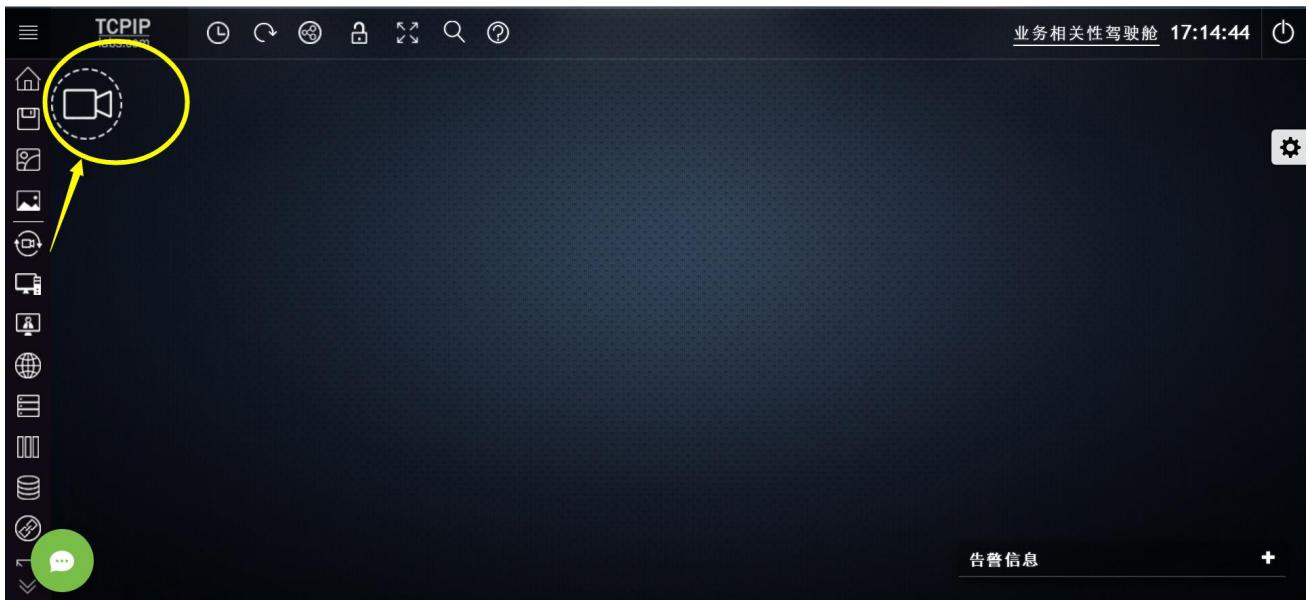
该功能在【监控对象设置】的最后一个功能，【驾驶舱管理与设置】。如下图：

| 驾驶舱名称 | 驾驶舱描述 | 创建用户 | 更新时间 | 状态 | 操作 |
|----------|-------|---------------------|------|----|----|
| 业务链驾驶舱 | leo | 2019-07-01 17:12:01 | 未锁定 | | |
| 业务相关性驾驶舱 | leo | 2019-08-08 00:55:47 | 未锁定 | | |

点击驾驶舱列表右上角的【+】，根据弹出窗口的提示，即可完成业务链驾驶舱的创建、修改和删除操作。

17.3.2. 如何添加，修改，删除业务链驾驶舱的内容？

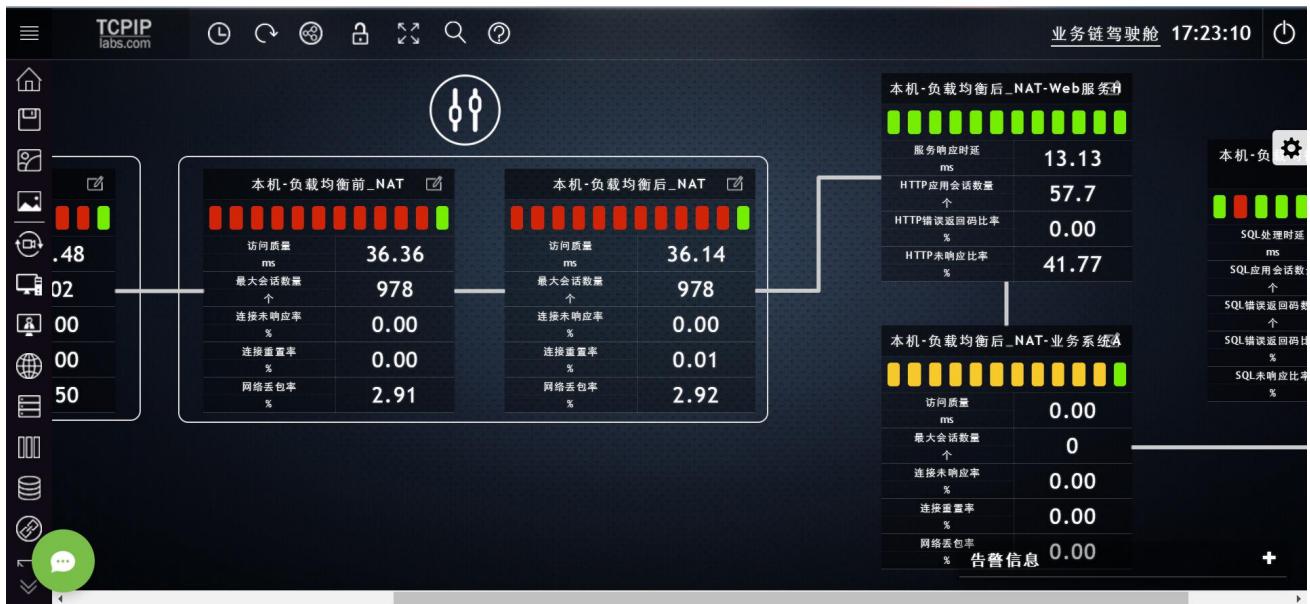
- 创建业务链驾驶舱后，用户需要刷新一次浏览器页面，即会在右侧主要功能栏的第一个图标【首页】弹出的菜单中，找到刚创建的新驾驶舱。点击该新建驾驶舱，即会进入该驾驶舱页面，如下图：
- 从左侧第 4 个图标开始，是可以添加的监控对象内容，添加监控对象图标后，如下图，双击该图标，会弹出监控对象的绘图列表，根据列表里的内容即可完成添加、修改和删除的进行设置。



- 双击监控对象图标后，弹出的绘图列表窗口如下图。选择数字形式会以小列表形式展示，图形形式会以线图、饼图等形式展示。



- 如何为不同监控对象的小列表添加连线？将鼠标放到每个小列表上下左右四个边缘的中间，即会出现一个小黑点，按住鼠标左键在小黑点上，并拖动到另一个监控对象小列表的边缘，即可完成连线操作。
- 重复如上操作，完成完整的业务链搭建过程。最终完成的样式可以参考下图：
- 如果要删除已经添加上去的内容？可以将鼠标放在该内容的右上角，即会出现删除功能【x】；



17.3.3. 业务链驾驶舱搭建要点提示

- 每次设置完一个监控对象内容，务必要点击【保存】功能！
- 不同部门，不同岗位的 XPM 用户，建议搭建符合自己应用场景的驾驶舱；并且，要在权限管理进行单独使用授权；
- 请严格按照业务链的逻辑进行搭建，只有这样做，才能在发生异常时，找到问题节点。例如，从左至右的监控对象小列表可以为：防火墙—>负载均衡—>Web 服务—>应用服务—>中间件—>数据库—>第三方应用；
- 每个小列表的 KPI/KQI 内容建议为：健康度，时延类 KQI，错误类 KQI，未响应类 KQI，会话数量；
- 页面上部的快捷工具栏的【时间回溯】功能，对业务链驾驶舱也有效，通过该功能，可以高效率的发现业务链上的异常节点。

18. 通信拓扑发现与梳理

通信拓扑发现与梳理，是 XPM 非常强大，实用和常用的功能之一，它的应用场景主要有

- 帮助用户验证业务链逻辑是否正确；
- 帮助用户发现网络中的活跃主机，或潜在风险主机；
- 帮助用户直观的判断每个 KPI/KQI 在不同主机间的大小，并钻取到通信对或会话。

18.1. 拓扑功能的基础操作

18.1.1. 拓扑功能的两个入口

- 页面右侧主要功能栏的【拓扑图】功能，该功能为拓扑发现；
- 页面上部快捷工具栏【拓扑查询】功能，该功能为拓扑梳理。

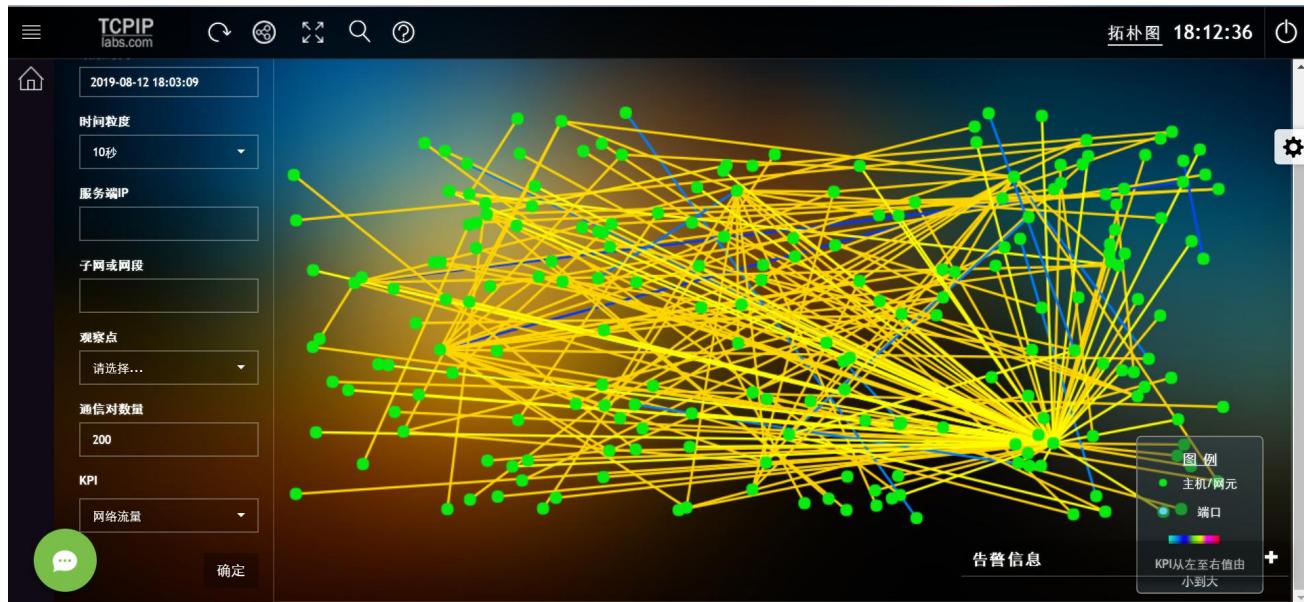
18.1.2. 拓扑功能的基础操作

- 拓扑图中的绿色圆点，代表 IP；蓝色圆点代表 Port；
- 双击绿色圆点（IP），可以钻取到 Port；再次双击 Port，可以进一步钻取到与之通信的 IP；这一操作
用来梳理业务链的路径！
- 连线的颜色，代表了 KPI/KQI 的数值大小，其图例在页面右下角；
- 双击两个 IP 圆点之间的连线，可以钻取到这两个 IP 之间的通信对；
- 滚动鼠标的滚轮，可以放大或缩小拓扑图；有助于更好的可视化效果；
- 在没有内容的空白区，按住鼠标左键，可以整体拖动拓扑图；
- 将鼠标光标放置在 IP 或 Port 圆点上，点击鼠标右键，可以弹出【复制当前 IP】，【删除对象】，【隐藏
工具栏】三个功能；
- 拓扑功能自带一个快捷工具栏，在拓扑图的右上角。快捷功能包括：框选，居中显示，保存状态，显
示/取消显示 IP，帮助，请求保存。

18.2. 如何使用拓扑发现功能

从首页页面右侧的【拓扑图】功能进入拓扑发现功能后，会呈现当前一分钟内，全网的通信拓扑关系。如

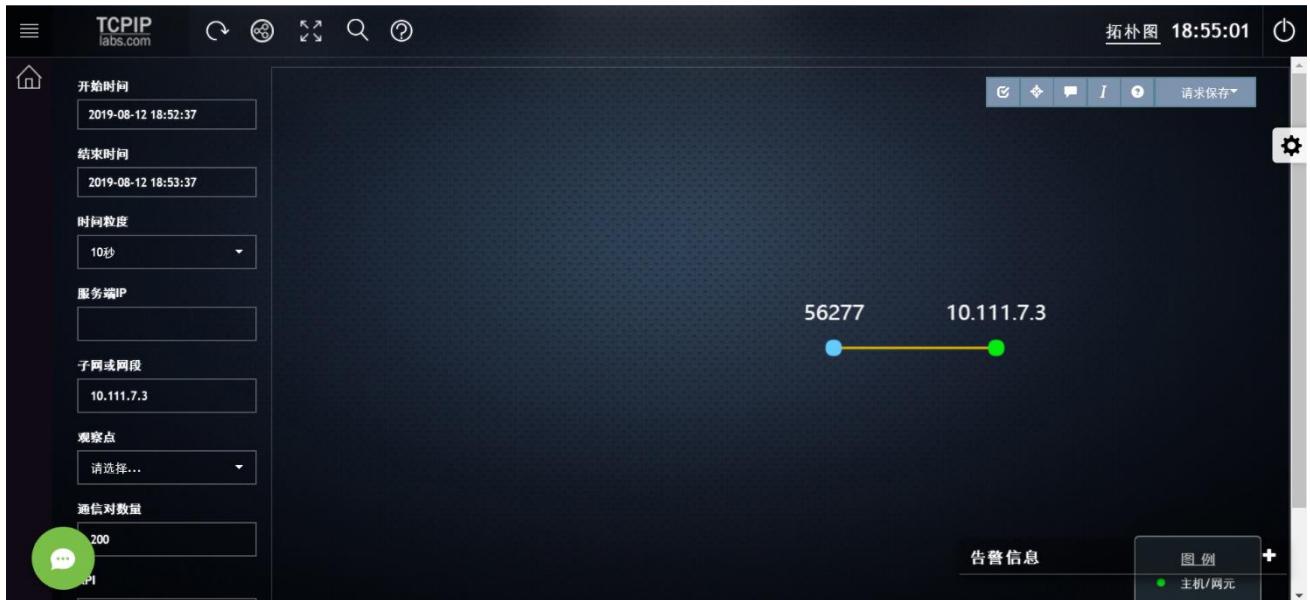
下图所示：



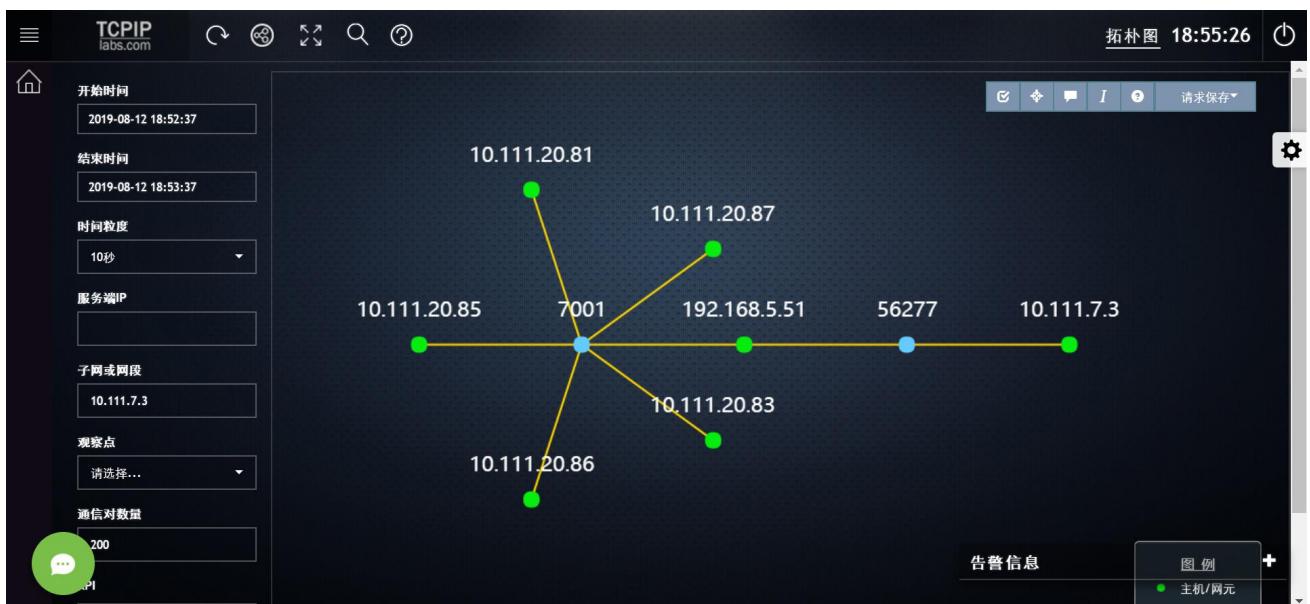
- 用户可以根据左侧的条件选择功能，对右侧的通信拓扑图进行定制化输出；
- 通信拓扑默认输出 200 个 IP，用户可以增加显示的数量，但显示的越多，拓扑输出的时间越长；
- 可以根据上一节中拓扑功能的基础操作，对拓扑图进行符合应用场景的各项操作。

18.3. 如何使用拓扑梳理功能

- 再次强调：通信拓扑梳理功能，可以用于验证业务链关系是否正确、准确，是 XPM 最重要的功能之一。
- 点击页面上部快捷工具栏的第 3 个功能，【拓扑查询】功能，即可进入拓扑梳理功能。
- 进入后，在左侧条件选择功能中，输入需要梳理的主机 IP，并逐一选择时间，KPI 类型，点击确定后，即可输出符合条件的第一个通信关系，如下图：



- 继续双击正在通信的端口 7001（蓝色圆点），并重复这一双击操作，即可梳理出一条完整的通信关系业务链；以该通信关系为依据，可以创建业务链驾驶舱，也可以验证业务部门提供的配置是否正确；



- 双击连线，可以获得相关通信的通信对。

The screenshot shows a table of communication pairs. The columns are '发起时间' (Initiation Time), '服务端IP' (Server IP), '客户端IP' (Client IP), '网络流量' (Network Traffic), and '连接发起数量' (Number of Connection Initiations). The data rows are:

| 发起时间 | 服务端IP | 客户端IP | 网络流量 | 连接发起数量 |
|---------------------------------|--------------|--------------|---------|--------|
| 08-12 18:53:10 ~ 08-12 18:53:30 | 192.168.5.51 | 10.111.20.87 | 17.78Kb | 4 |
| 08-12 18:53:10 ~ 08-12 18:53:30 | 192.168.5.51 | 10.111.20.87 | 17.78Kb | 4 |
| 08-12 18:52:40 | 192.168.5.51 | 10.111.20.86 | 11.11Kb | 2 |
| 08-12 18:52:40 | 192.168.5.51 | 10.111.20.86 | 11.11Kb | 2 |
| 08-12 18:53:00 | 192.168.5.51 | 10.111.20.81 | 8.58Kb | 2 |
| 08-12 18:53:00 | 192.168.5.51 | 10.111.20.81 | 8.58Kb | 2 |

19. 流量存储与回溯

流量回溯与分析（以下简称 TSE），是 XPM-H 的重要功能之一，XPM-S 和 XPM-V 不提供此功能。

TSE 的原理是以高性能无损技术，将网络流量存储在本地磁盘阵列，并在发生疑难的安全或运维事故后，通过 TCP/UDP 五元组将事故原始流量提取出来，使用本地数据包解析工具（例如 Wireshark）打开并进行详细剖析。

由于 TSE 存储的是完整的，未经任何处理的网络流量，所以 TSE 也是最有效，最可靠的一种数据还原取证方法，在很多时候，甚至是唯一的技术手段。

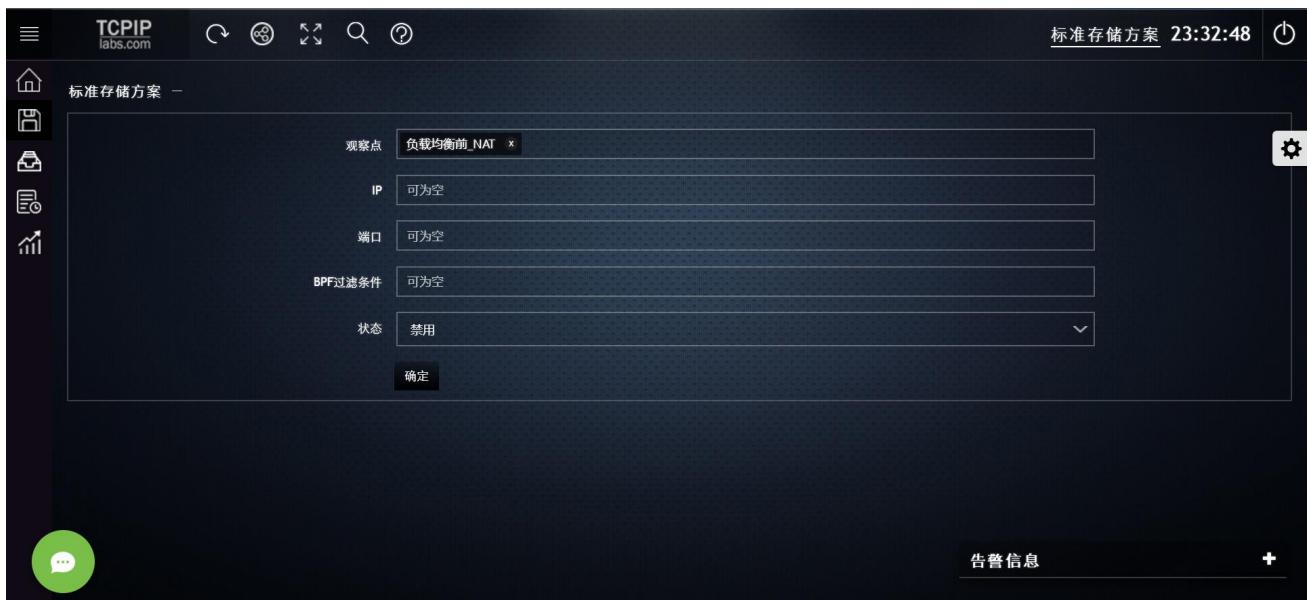
在安全和运维理论中，TSE 是安全和运维体系的最后一道技术保障措施，也是安全和运维架构形成闭环的最后一个环节。

19.1. XPM 流量存储与回溯功能的特点

- 对 XPM-H 版本，在满足硬件建议标准的前提下，XPM-H 可以提供高达 16Gbps 的零丢包无损存储能力；
- 通过告警或图形钻取到通信对或会话列表，并最精确、精简的数据包，有效降低离线分析工作量；
- 在指定五元组条件后，可以从 TB 级别原始流量中，以秒级速度提取符合条件的原始数据包；
- 提供高级存储方案，有效节省用户存储资源。

19.2. 流量存储的功能入口

流量存储的入口只有一个，即：页面左侧的主要功能栏的第 4 个功能。点击进入后，功能页面如下图：



19.3. 标准存储方案

提供对观察点，或 IP，或端口的存储方案；同时支持 BPF 过滤条件。



19.4. 高级存储方案

点击流量存储功能左侧第 3 个功能【高级存储方案】，即可进入该功能页面：



创建一个新的高级存储策略，在列表右上角第 3 个功能【+】新增功能；点击【+】后，会弹出如下窗口：



根据该窗口中的各个功能选项，用户可以订制存储条件包括：方案生效时间，截包大小，以及其他标准存储方案里的条件。

19.5. 历史数据提取（流量回溯）

流量回溯的功能入口有两个。

- 一个是在如上截图中，左侧功能栏的第 4 个功能【历史流量提取】；
- 另一个是在每个通信对或会话列表的右上角的下载功能【】，点击该功能后，根据提示，用户可以将该通信的原始流量，以 PCAP 文件格式下载到本地，并用 Wireshark 等数据包解析工具打开并做进一步分析。

19.6. 数据提取列表

- 对于已经提取的原始数据包，XPM 会存储一个备份在本地存储单元，如果用户需要再次提取，可以使用此功能。

| 文件名称 | 类型 | 文件大小 | 时间 | |
|-------------|-----|---------|---------------------|---|
| 1560583945 | 文件夹 | 3.02Kb | 2019-06-15 15:32:32 |  |
| 1560583771 | 文件夹 | 18.34Kb | 2019-06-15 15:29:37 | |
| huya.pcapng | 文件 | 2.59Mb | 2017-06-22 18:06:39 | |

20. 主要功能与应用场景

20.1. 对业务/应用/网络性能异常的预警和定位

对业务/应用/网络的性能预警，就是要对与业务/应用/网络有关的性能指标 KQI 进行合理的阈值设置，并在达到阈值时触发告警；相关问题和流程，请按照如下顺序理解：

- A. 这些性能指标 KQI 详见：[XPM 的 KPI 和 KQI 都有哪些？](#)，
- B. 每种性能指标都代表了哪些故障域方向：[性能指标 KQI 的解释与故障域方向](#)
- C. 告警的设置方法详见：[告警阈值设置的功能入口](#)，
- D. 阈值的范围请详见：[如何合理的设置性能指标 KQI 的告警阈值。](#)
- E. 如何及时的获得告警信息，并钻取到通信对或会话，请详见：[告警信息获取和钻取](#)

20.2. 性能可视化监控（上屏监控）

XPM 的 UI 设计已经充分考虑了上屏监控的需求，因此在界面的美观性，灵活性方面，都有专门的设计。具体可通过业务链驾驶舱实现，请详见：[业务链驾驶舱](#)

20.3. 统计分析业务/应用/网络的运行规律与关联关系

- 如何在相同类型的监控对象中，找到性能最差的监控对象？

通过统计分析驾驶舱的列表功能，并回溯需要统计分析的时间段，用户可以对同类型监控对象的不同群组进行对比分析，找到处理性能最劣化的 Web 服务，或 SQL 返回码最多的 DB 服务，或访问质量最劣化的分支机构，或链路时间消耗最多的观察点。

- 如何掌握会话量与服务性能的运行规律和关联关系？

在统计分析驾驶舱，通过在列表第一列，选择不同的监控对象，可以改变列表下面的图形内容，结合时间回溯，则可以发现业务，应用和网络各个 KQI 之间的关系，例如：

- A. 当 TCP 通信量峰值的时候，握手时延是多少？
- B. 当 HTTP 会话量峰值的时候，Web 的处理性能是多少？
- C. 当 DB 处理时延最高的时候，处理时延的 TOP 10 是哪些 SQL？

20.4. 如何定位网络串行设备的时延

网络串行设备包括交换机，防火墙，负载均衡，各类安全设备；这些设备对网络质量的性能消耗，是网络运维工作中较难定位和排查的常见问题；

在 XPM 中，定位这类时延或错误的网络瓶颈较为简单，只需要在搭建好的业务链驾驶舱，进行时间回溯，并通过对不同监控对象之间，相同性能指标的差值，即可找到是哪个监控对象，或哪个网段出现了性能下降。

20.5. 如何界定用户投诉的故障域范围

如果加载了 HTTP 模块，且每个观察点都可以看到 HTTP 流量，则通过搜索投诉的【客户端 IP】，和业务所包含的【URL】，即可找到该客户端 IP 的所有投诉时段的 HTTP 会话，然后，通过对比同一条 HTTP 会话的 KQI 时延，在不同观察点间的时间损耗，即可定位故障域范围。如下图：

| 开始时间 | 结束时间 | 观察点名称 | 服务端IP | 客户端IP | URL | 命令类型 | HTTP返回码 | URL负载传输时延 |
|----------------|----------------|-----------|--------------|---------------|-------------------------------|------|---------|-----------|
| 08-17 01:02:59 | 08-17 01:02:59 | 负载均衡后_NAT | 192.168.1.12 | 192.168.1.106 | 192.168.1.12/ipmOracleServlet | POST | 200 | 49.08ms |
| 08-17 01:02:59 | 08-17 01:02:59 | 负载均衡前_NAT | 192.168.1.12 | 192.168.1.106 | 192.168.1.12/ipmOracleServlet | POST | 200 | 49.82ms |
| 08-17 01:02:37 | 08-17 01:02:39 | 负载均衡后_NAT | 192.168.1.12 | 192.168.1.106 | 192.168.1.12/ipmOracleServlet | POST | 200 | 2008.71ms |
| 08-17 01:02:37 | 08-17 01:02:39 | 负载均衡前_NAT | 192.168.1.12 | 192.168.1.106 | 192.168.1.12/ipmOracleServlet | POST | 200 | 2008.12ms |
| 08-17 01:02:29 | 08-17 01:02:29 | 防火墙前 | 192.168.1.12 | 192.168.1.106 | 192.168.1.12/ipmOracleServlet | POST | 200 | 33.42ms |
| 08-17 01:02:29 | 08-17 01:02:29 | 防火墙后 | 192.168.1.12 | 192.168.1.106 | 192.168.1.12/ipmOracleServlet | POST | 200 | 32.68ms |

20.6. 对流量异常的预警和分析

异常流量的预警和分析，是网络运维和安全部门的工作难点之一。在 XPM 中，我们可以按照如下流程进行操作：

设置合理的智能预警阈值范围，详情参见：[如何合理的设置状态指标 KPI 的告警阈值](#)

获得告警信息后，先钻取到告警图形，然后，通过拖拽形成异常的波峰或波谷，即可钻取到导致波峰或波谷的通信或会话，请详见：[告警信息获取和钻取](#)

20.7. 如何对网络流量进行多维度分析

通过 XPM 的聚合分析功能，用户可以实现各种维度、任意时间、任意 KPI 的累计或平均值统计分析。

操作路径：【需要分析的 KPI/KQI 线图】→进入该线图页面，左侧默认为【聚合分析维度】→在输入框中填写各项条件后，点击确认 → 得到图形，再根据时间轴，拖拽，即可得到该段时间内，分析对象的各维

度统计分析值。

聚合分析功能非常强大！它不仅提供了丰富的统计分析维度，还独创了“聚合”概念，并且，所有统计分析内容，都可以在短短几秒中获得，即使是长达数天的统计需求。

| 发起时间 | 服务端IP | 客户端IP | 网络流量 | TCP连接发起 |
|---------------------------------|---------------|--------------|--------|---------|
| 11-10 03:50:00 - 11-11 03:30:00 | 1.245.177.220 | 10.70.73.113 | 2.19Mb | 3,910 |

长达一天时间，对某IP的统计分析

20.8. 如何给出有针对性的优化建议

运维部门可以通过 XPM 的 HTTP 模块，DB 模块的分析功能，帮助运维部门向研发部门提出有针对性的优化建议。例如：

- 最慢 URL，错误返回码最多的 URL；
- 最慢 SQL，返回码最多的 SQL。如下图：

| 开始时间 | 结束时间 | 观察点名称 | 服务端IP | 客户端IP | URL | 命令类型 | HTTP返回码 | URL负载传输时延 | 响应时延 |
|----------------|----------------|-----------|--------------|---------------|--|------|---------|-----------|------|
| 08-17 01:50:43 | 08-17 01:50:43 | 负载均衡前_NAT | 192.168.1.12 | 192.168.1.121 | 192.168.1.12/ipmapDb2Servlet | POST | 0 | <1ms | <1 |
| 08-17 01:50:42 | 08-17 01:50:42 | 负载均衡前_NAT | 192.168.1.12 | 192.168.1.121 | 192.168.1.12/ipmapDb2Servlet?aim=getDb2Chenk | POST | 0 | <1ms | <1 |
| 08-17 01:50:42 | 08-17 01:50:42 | 负载均衡前_NAT | 192.168.1.12 | 192.168.1.121 | 192.168.1.12/ipmapDb2Servlet | POST | 告警信息 | <1ms | <1 |
| 08-17 01:50:58 | 08-17 01:50:58 | 负载均衡前_NAT | 192.168.1.12 | 192.168.1.121 | 192.168.1.12/ipmapDb2Servlet | POST | 0 | <1ms | <1 |



附件 1：指标算法说明

XPM 全栈性能管理与流量分析平台

指 标 算 法 说 明

Ver 4.0

2019 年 8 月

1. 观察点/服务端/客户端

| KPI | 描述 | 单位 |
|----------|---------------------------------|-----|
| 访问质量 | 两端握手+应用处理+负载传输 | ms |
| 服务端通信时延 | 发送给服务端数据到收到服务端[ACK]的时间差 | ms |
| 客户端通信时延 | 发送给客户端数据到收到客户端[ACK]的时间差 | ms |
| 链路时延 RTT | 服务端通信时延 + 客户端通信时延 | ms |
| 服务端握手时延 | 发送给服务端[SYN]到收到服务端[SYN, ACK]的时间差 | ms |
| 客户端握手时延 | 发送给客户端[SYN, ACK]到收到客户端[ACK]的时间差 | ms |
| 应用处理时延 | 第一个请求包到第一个响应包的时间差 | ms |
| 负载传输时延 | 第一个响应包到最后一个响应包的时间差 | ms |
| 服务端重传时延 | 发送给服务端的最后一个重传包与发送包的时间差 | ms |
| 客户端重传时延 | 发送给客户端的最后一个重传包与发送包的时间差 | ms |
| 网络流量 | 统计数据帧流量大小（二层流量） | bps |
| TCP 流量 | 3 层协议字段为 tcp 的数据帧的流量 | bps |
| UDP 流量 | 3 层协议字段为 udp 的数据帧的流量 | bps |
| 下行流量 | 目的 IP 在内网网段设置里的所有流量 | bps |
| 上行流量 | 源 IP 在内网网段设置里的所有流量 | bps |
| 未定义服务端流量 | 源或目的地址不在已定义的服务端范围内的流量 | bps |
| 未定义客户端流量 | 源或目的地址不在已定义的客户端范围内的流量 | bps |
| 最大会话数量 | 一段时间内活跃的 TCP/UDP 连接数量中最大个数 | 个 |
| 连接发起数量 | 单 SYN 包的数量 | 个 |
| TCP 连接重置 | 带 RST 包的数量 | 个 |
| 连接响应数量 | 带 SYN/ACK 包的数量 | 个 |
| 连接关闭数量 | 带 FIN 包的数量 | 个 |
| 主动关闭连接数量 | 四路中断中第一个 FIN 包的数量 | 个 |
| 连接未响应率 | 有 SYN, 无 SYN/ACK 的包的数量 | 个 |
| 被动关闭连接数量 | 四路中断中第二个 FIN 包的数量 | 个 |
| 数据包速率 | 统计二层数据包速率 | pps |

| | | |
|----------------|---------------------------|-----|
| 网络丢包率 | 重传包数 / TCP 总包数 | % |
| 服务端丢包率 | 服务端收到重传包数 / 服务端收到 TCP 总包数 | % |
| 客户端丢包率 | 客户端收到重传包数 / 客户端收到 TCP 总包数 | % |
| 小包速率 | 包长度小于 64 的包速率 | pps |
| 小包比率 | 小包数 / 总包数 | % |
| 平均包长 | 总字节数 / 总包数 | |
| 零窗口包数 | 源或目的窗口为零包数 | 个 |
| 上行带宽占用率 | 上行网络流量 / 上行带宽 | % |
| 下行带宽占用率 | 下行网络流量 / 下行带宽 | % |
| ARP 流量 | ARP 的统计流量 | bps |
| ARP 包速率 | ARP 的包速率 | pps |
| 连接重置率 | RST 包数 / 会话数量 | |
| 会话数量 | 活跃的 TCP/UDP 连接数量 | 个 |

2. HTTP 服务

| KPI | 描述 | 单位 |
|---------------------|---|-----|
| 服务端通信时延 | 针对每一条 HTTP 会话，客户端发送应用层数据最后一个数据包，服务器端对该数据包确认的时间差 | ms |
| 客户端通信时延 | 针对每一条 HTTP 会话，服务端发送应用层数据最后一个数据包，客户端对该数据包确认的时间差 | ms |
| 链路时延 RTT | 服务端通信时延 + 客户端通信时延 | ms |
| 服务响应时延 | 针对于每条 http 会话，请求第一个数据包与相应第一个数据包时间差 | ms |
| URL 负载传输时延 | 针对于每条 http 会话，请求第一个数据包与相应最后一个数据包时间差 | ms |
| 网络流量 | 针对定义的 ip: port 的流量，包括源和目的。 | bps |
| HTTP 应用会话数量 | HTTP 应用会话的条数 | 个 |
| HTTP 错误返回码比率 | HTTP 错误返回码数量 / HTTP 应用会话数量 | % |
| HTTP 未响应比率 | HTTP 未响应数量 / HTTP 应用会话数量 | % |
| 网络通信丢包率 | 针对定义的 ip: port 的重传包 / 总包数 | % |

3. Oracle/MySQL/SQLserver

| KPI | 描述 | 单位 |
|--------------------|--|-----|
| 服务端通信时延 | 针对每一条 SQL 会话，客户端发送应用层数据最后一个数据包，服务器端对该数据包确认的时间差 | ms |
| 客户端通信时延 | 针对每一条 SQL 会话，服务端发送应用层数据最后一个数据包，客户端对该数据包确认的时间差 | ms |
| 链路时延 RTT | 服务端通信时延 + 客户端通信时延 | ms |
| SQL 处理时延 | 针对于每条 SQL 会话，请求第一个数据包与相应第一个数据包时间差 | ms |
| SQL 服务流量 | 针对定义的 ip: port 的流量，包括源和目的。 | bps |
| SQL 应用会话数量 | SQL 应用会话的条数 | 个 |
| SQL 错误返回码数量 | 返回码为非 0 的会话的个数 | 个 |
| SQL 错误返回码比率 | SQL 错误返回码数量 / SQL 应用会话数量 | % |
| SQL 未响应数量 | 超过 60 秒无响应的 SQL 应用会话的条数 | 个 |
| SQL 未响应比率 | SQL 未响应数量 / SQL 应用会话数量 | % |
| 网络通信丢包率 | 针对定义的 ip: port 的重传包 / 总包数 | % |