前言

网络监控管理是 IT 监控和运维管理中不可缺少和基础性的内容，也是相当成熟的监控管理领域，包括成熟的方案，产品和市场等。但是随着大数据，云计算和人工智能的急剧发展，面向基础架构，云计算以及应用等资源的一体化的运维和监控平台需求越来越迫切，传统的产品和手段因其技术局限性，功能单一，信息孤岛等缺点而不能满足以上要求。而基于现代化技术设计，并经过大规模实践验证的蓝鲸智云以其 PaaS 平台架构，通过“蓝鲸+”体系，能够打造全面覆盖网络，计算，存储，云，中间件和应用等方面的监控管理平台。为此，我们推出了这个开箱即用，高度自动化的网络管理平台，从而进一步极大的丰富了 **“蓝鲸+”** 体系。

产品简介

网络监控管理是 IT 监控和运维管理中不可缺少和基础性的内容，也是相当成熟的监控管理领域，包括成熟的方案，产品和市场等。但是随着大数据，云计算和人工智能的急剧发展，面向基础架构，云计算以及应用等资源的一体化的运维和监控平台需求越来越迫切，传统的产品和手段因其技术局限性，功能单一，信息孤岛等缺点而不能满足以上要求。而基于现代化技术设计，并经过大规模实践验证的蓝鲸智云以其 PaaS 平台架构，通过“蓝鲸+”体系，能够打造全面覆盖网络，计算，存储，云，中间件和应用等方面的监控管理平台。为此，我们推出了这个开箱即用，高度自动化的网络管理平台，从而进一步极大的丰富了 **“蓝鲸+”** 体系。

“网络管理” 是一款面向网络设备的开箱即用的监控平台。具有全网设备及其模块自动发现，异构网络环境物理拓扑自动发现，日志事件的自动采集及自动处理，多设备多 KPI 性能数据的任意组合展现等功能和特色。该应用为运维人员提供了简洁、直观、易用的网络设备监控手段。该社区版应用的主要功能和特色有：

- 网络设备和服务器(支持 snmp)及其设备模块的自动发现，包括设备类型和模块类型的自动判断和归档；支持 SNMP v1,v2,v3。
- 异构网络设备环境，物理拓扑图的自动发现。采用了 FDB,STP, CDP 等多种发现方式，以确保完整准确发现全网设备的物理拓扑
- 能自动发现服务器和交换机之间的物理拓扑连接
- 日志事件的自动采集和事件的抑制、压缩、丰富、自愈、转发、合并、升降级等处理
- 支持低级别事件的自动降级处理，从而可以抑制不必要的事件
- 预置常见的性能 KPI 指标，新增设备无需定义 KPI，即会自动采集常用的性能指标数据
- 多设备、多端口、多 KPI 性能数据可以任意组合展现

术语解释

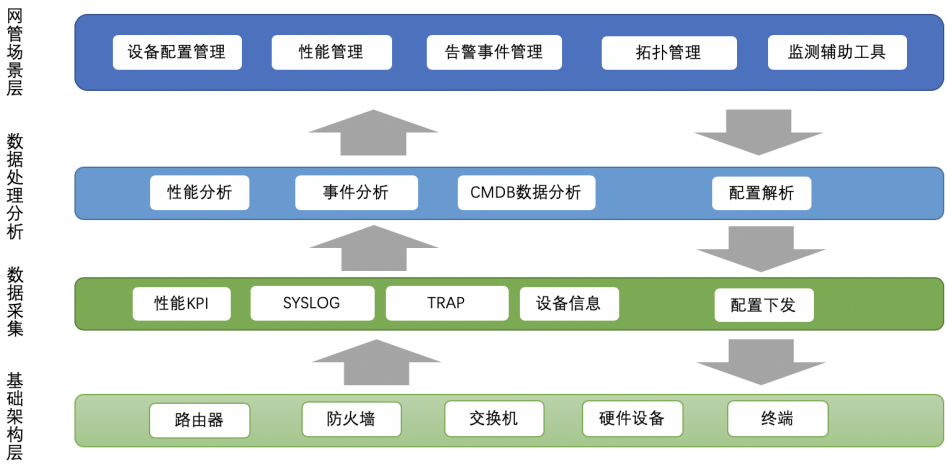
术语	解释
设备(Device) 节点(Node)	指网管系统能够管理到的网络中的节点，如路由器、交换机、防火墙、主机等。他们能够发出 Syslog 信息，或支持 SNMP read，或支持 ping 等操作，使得网管系统可以获取其有关的状态 信息（实时或非实时的信息)。设备也称为节点(Node)
线路(Line)	线路定义为两个物理设备的各自一个端口之间的物理连接，由一个本段端口和一个对端端口 确定。可分为局域网线路和广域网线路，本系统一般仅关注广域网线路（如果没有特别说明， 线路指广域网线路）。 从业务上看，线路可以分为分支机构线路、银行线路、Internet 线路、 第三方线路等。**线路由本端端口（如上海某路由器的端口）和对端端口（北京某路由器端口） 确定**
事件(Event)	任何一个有关设备或线路状态的信息称为事件。事件信息有两个来源： 1）设备自动送出的 Syslog 或 Trap； 2）网管系统主动去轮询设备的指定信息（如当前的 CPU 利用率）后，经分析计算认为超过或低于标准值而产生的事件信息。 事件的严重等级一般定义成 5 级，见下一章节"事件等级定义"事件的主要信息包括：IP 地址、信息内容、首次发生时间、最近 一次发生的时间、事件等级、事件类型。
故障(Fault)	指严重的事件。一般根据业务而定，如将 5 级事件称为故障。自愈(对冲)(Offset)同一设备的两个同样类型、而方向相反的事件之间相互抵消称为对冲。 如: rp001 设备的 FastEther1/0/9 端口出现一个 Link Down 事件，5 秒钟后，该设备的同一端口出现 Link Up 事件，那么网管系统在几秒左右之后，会在后台将这两个事件记录相互抵消，而监控图上则 1 分钟左右之后会自动清除。所以用户有可能从实时监控图上看不到这些事件。但可以通过其他功能或报表了解到。对冲使（自愈）得这些事件得到了自动化处理，简化了人工处理和减少了事件的信息量。
管理地址(Management IP)	设备发出 Syslog 或 Trap 信息时，所代表该设备的 IP 地址。在本网管系统中，除特 别说明外，IP 地址指管理地址。
部门/区域代码	监控图和管理功能一般根据设备或线路所处的区域划分来进行监控和处理。如全国监控图分为个省市区域，总部监控图分为各网络区域。系统将每个分支机构和总部的各区域进行代码 化；如 HQ-PD-FLOOR 代表总部浦东区的楼层区。BJ-BXL 表示北京某地的分支机构。
事件丰富	将设备或线路资产的某些信息附加的事件记录中去，使得事件信息更加完整和容易处理。如将线路的对端端口的单位名称、设备名称和负责人的信息附加到事件记录后，监视人员或网管人员就能方便的找到联系人。
事件列表(AEL)(Active Event List)	以表格的形式显示设备或线路的事件信息。如设备事件列表显示的主要内容有：设备所属部门、设备名称、IP 地址、发生次数、首次获得最新发生时间、事件类型、摘要、联系人信息。事件等级是通过颜色表示的。系统内置了一个简单的 case 处理流程，包括分配，挂起，正常关闭，忽略，快速关闭。

事件(故障)等级定义

事件等级	英文名称	中文名称	颜色
5	Critical	严重	红色
4	Major	重度	橘黄色
3	Minor	中度	黄色
2	Warning	轻度	蓝色
1	Indeterminate	不确定	紫色
0	Clear/Normal	正常	绿色

产品架构图

网管社区版通过基于 SNMP 协议，对基础架构层的网络设备进行性能、Syslog、Trap 和设备信息的采集。经由后台处理分析后入库并展示给上层用户，供用户进行各场景的使用。 对于某些辅助功能，如配置下发，ping 工具等，则通过 SSH，TELNET 或者 PING 工具对纳管的设备进行数据传输和下发。



功能介绍

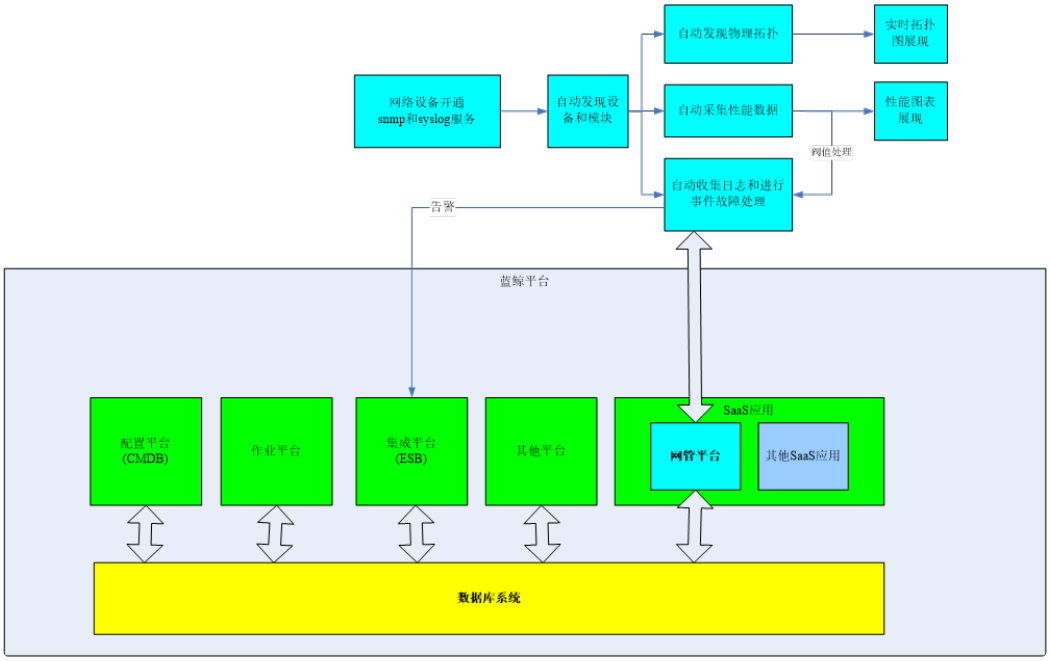
社区版的主要功能包括：

- 设备管理：设备和模块信息的自动扫描和归档。
- 事件和故障管理：事件丰富、压缩、对冲、关联和自动化等处理
- 性能管理：海量性能 KPI 数据的采集，阀值处理和多 KPI 的自由组合展现
- 拓扑管理：异构网络环境的物理拓扑自动发现和动态展现
- 监控对象包括但不限于：网络设备，安全设备，服务器等。

核心优势

社区版做为蓝鲸平台的一个 SaaS 应用，与蓝鲸平台紧密结合，包括：

- 一体化部署：随着蓝鲸平台的部署而自动完成安装和启动运行
- 单点登录：集成蓝鲸平台的用户和权限管理体系
- 告警服务：集成蓝鲸的告警平台
- 可以集成蓝鲸平台的 CMDB



自动发现

产品支持所需的各种处理的自动工作，无需手工去增添资源信息。这些自动化工作包括但不限于：

- 设备的自动发现
- 设备类型的自动判断和归档
- 设备模块的自动发现和类型自动判断
- 设备发现后自动采集基本的性能数据
- 异构环境的网络物理拓扑的自动发现
- 日志信息的自动采集和抑制，丰富，升降级，自愈，转发等自动处理

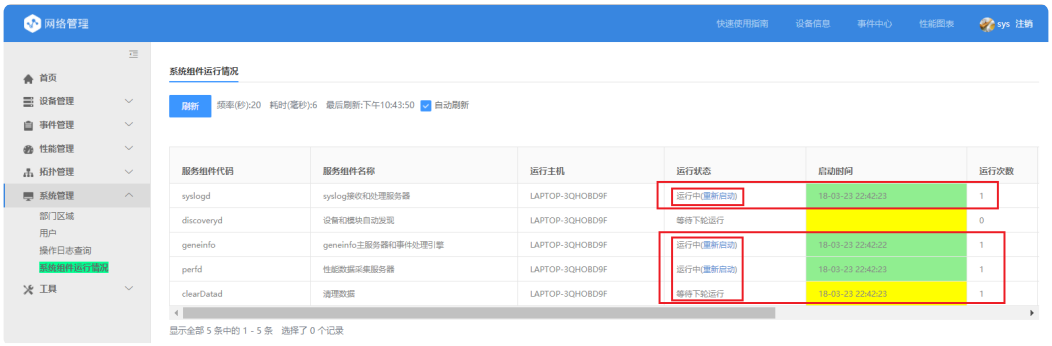
开箱即用

产品预置了系统运行所需的基本参数，包括设备类型定义，KPI，设备分组，常用性能数据采集插件等。系统初次运行之后，即可进行设备的自动扫描，性能数据的自动采集，日志事件的自动采集和处理等，无需手工配置。

如何开始

系统已内置了必要和常见的各种参数，系统基本上开箱即用。登陆后，点击上面的 “快速使用指南”，如下图所示，根据指南的 4 个步骤描述基本上就完成了整个网络管理的任务。

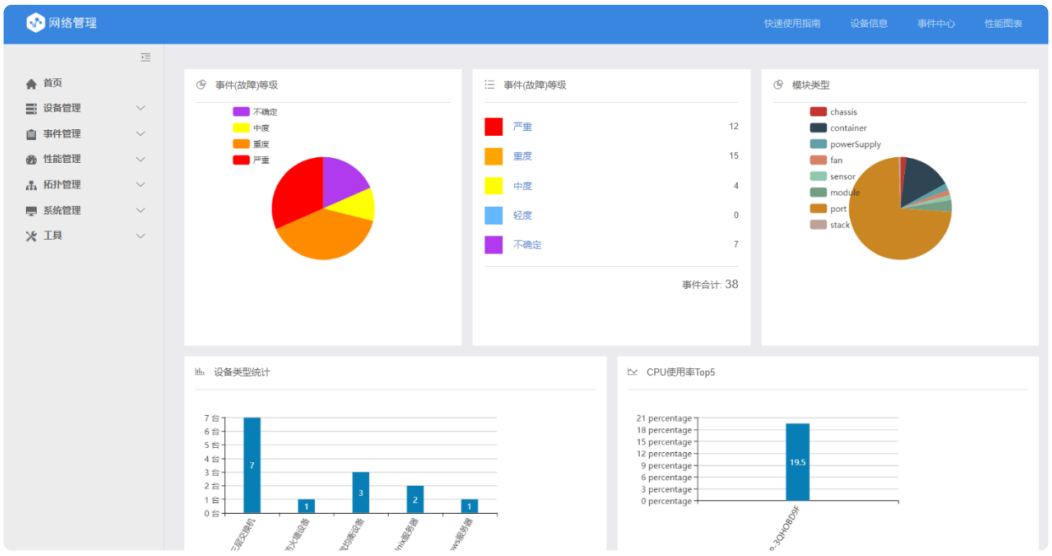
首先我们确认以下组件运行正常：



其次，第二步要去开通网络设备的 SNMP 和 Syslog 服务。

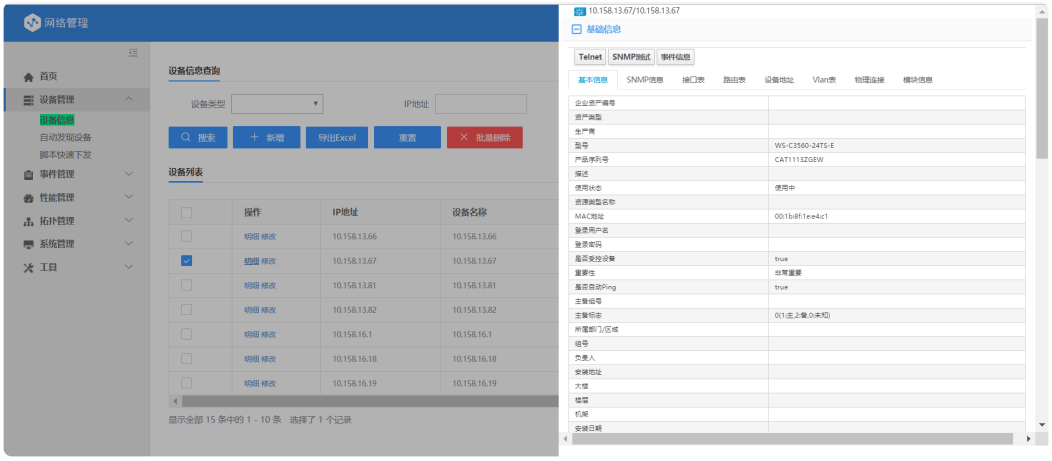
主页

主页集中展现了设备，事件和关键性能 KPI 的信息。点击【事件(故障)等级】各项，可以查询到到事件中心的相应事件明细信息。



设备信息操作

支持组合查询方式：



批量导入：”设备信息”--”新增”-”批量导入”

自动发现设备

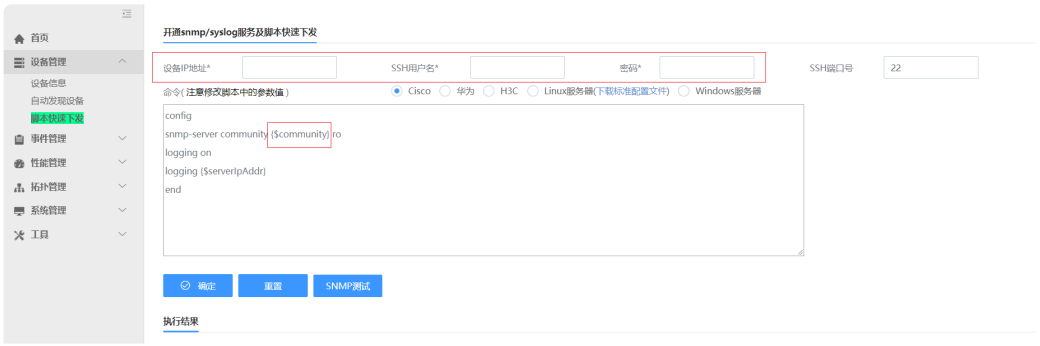
最少输入 “开始 IP 地址” 和 Commonity 即可。提交后，显示以下进度信息：

- 各设备连通性情况：**意味设备需要 ping 的通**。
- SNMP 支持情况：**意味设备需要支持 SNMP**。
- SNMP 信息采集情况。
- 识别出来的设备类型。
- 设备信息保存情况。

设备 SNMP 和 Syslog 的开通及脚本快速下发

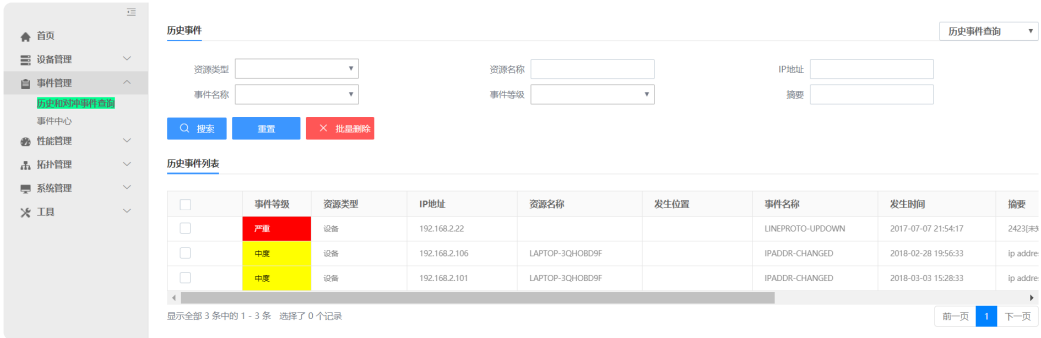
被管设备需要支持 SNMP。事件（故障）管理是根据采集的 Syslog 进行处理，系统以 deamon 方式等待采集来自设备送过来的 Syslog，因此网络设备和其他被管设备需要开通 Syslog 和设置 Syslog 的接收目的地。

下图“脚本快速下发”功能能够完成设备的以上配置（**注意这是个高风险操作，要谨慎操作**）



历史和对冲事件查询

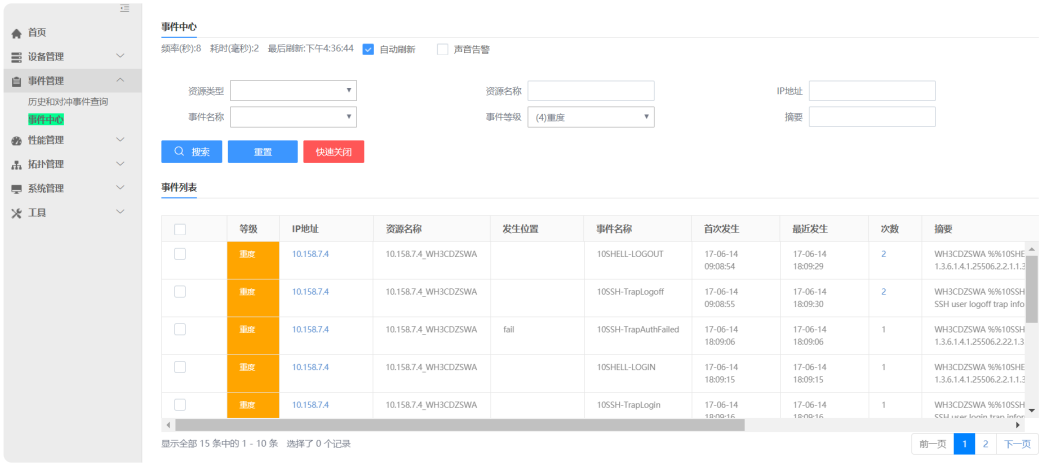
历史事件和对冲（自愈）事件可以选择 “历史和对冲事件查询” 菜单：



事件中心和其他事件信息的查询

事件中心集中展现了纳管设备的状态和发生的各种事件（故障）信息，应该是整个系统中最重要的功能，也是管理员最关注的地方。

事件管理包括抑制，丰富，对冲（自愈），转发，升降级等处理，可以最大程度地实现“不错发”、“不漏发”、“及时报”的故障管理目标。事件信息来源于收到和分析后的 syslog，以及阀值信息。



性能图表

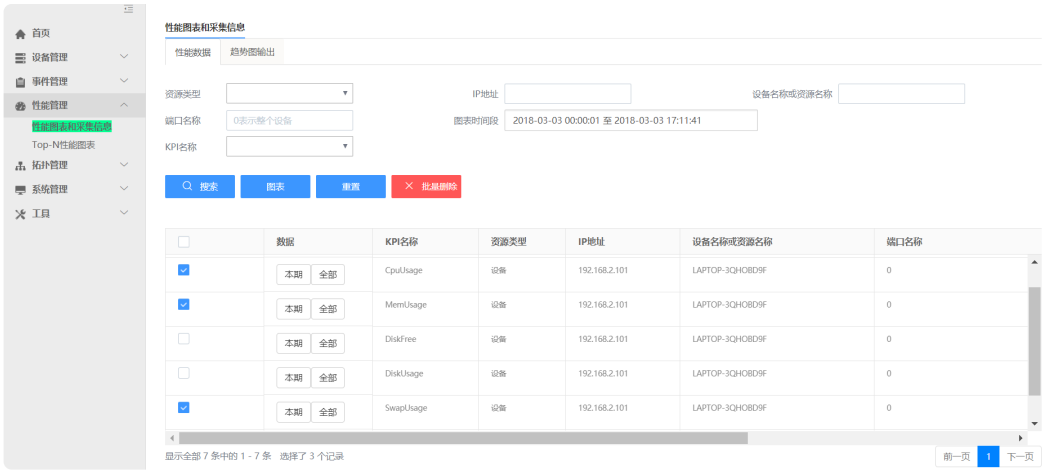
系统内置支持采集网络设备的以下 KPI：

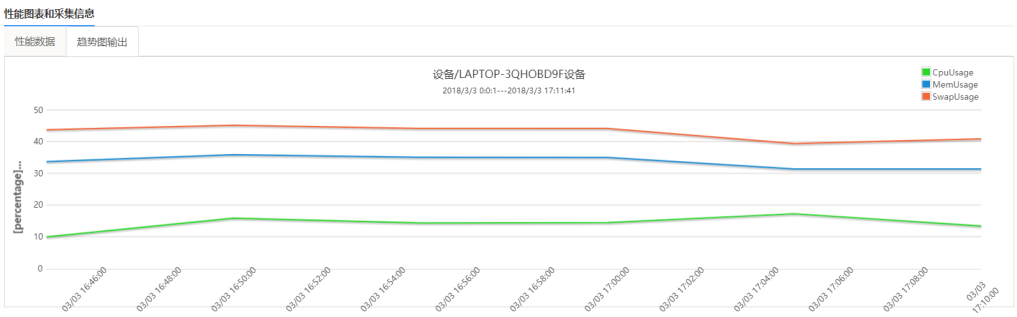
- 内存利用率
- CPU 利用率
- 端口流量

内置支持采集 Linux，Windows 服务器（已配置 snmp）的以下 KPI：

- CPU 利用率
- 内存利用率
- 端口流量
- 磁盘利用率
- 磁盘 IOPS

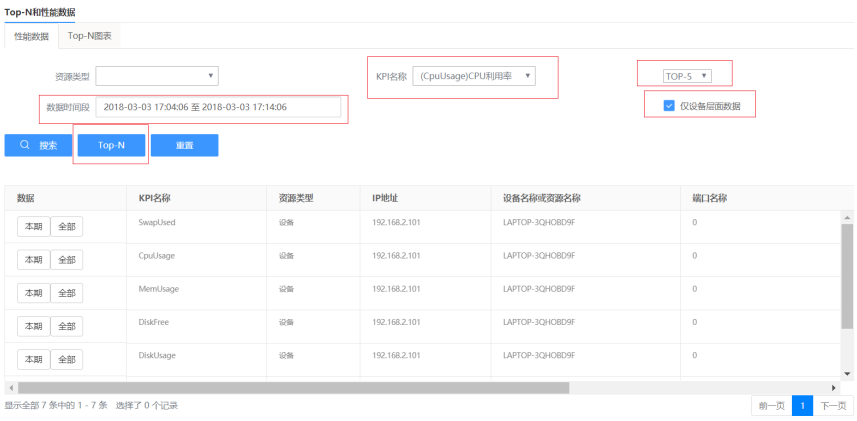
可以将不同设备，不同端口，不同 KPI 的数据任意组合在一起展现，从而可以进行各种横向比较，如下图所示：

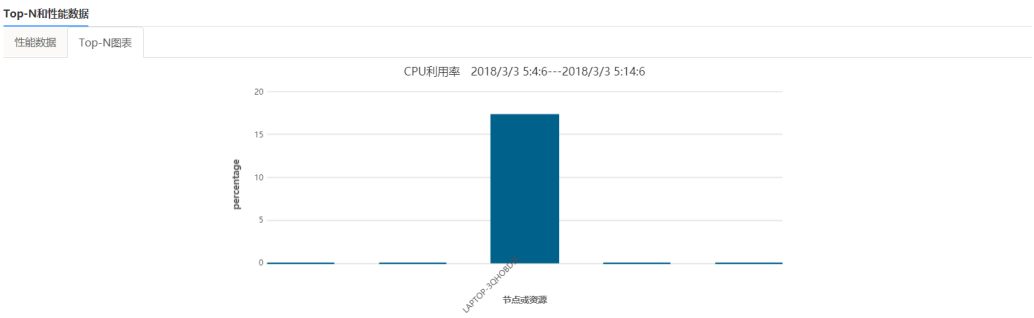




Top-N 性能图表

Top-N 则展现了同一 KPI，不同设备或不同端口的性能值比较：

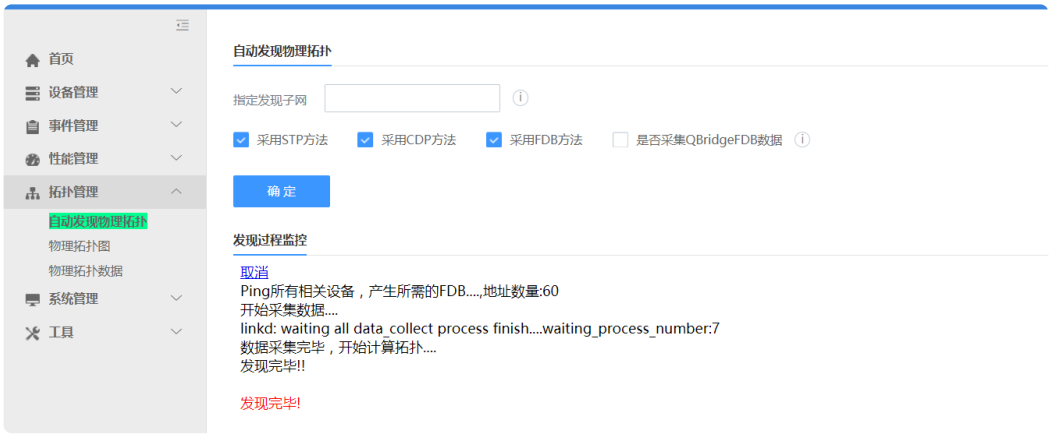




自动发现物理拓扑

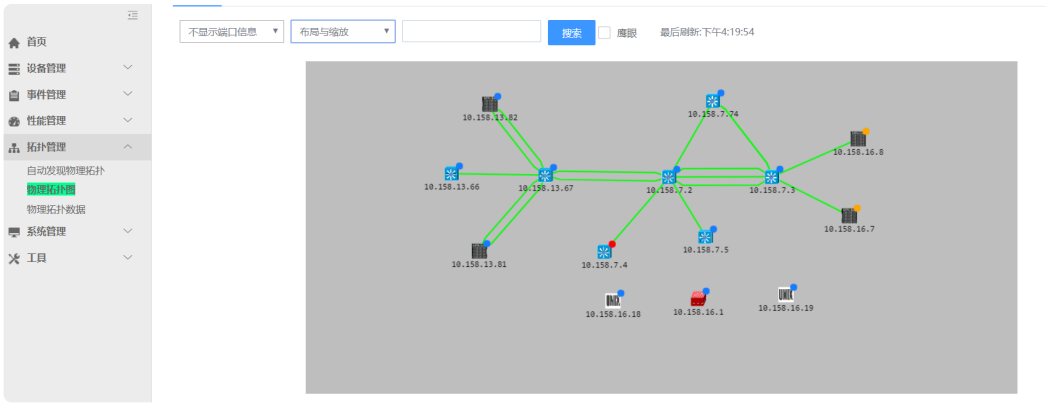
一般直接点击“确定”开始物理拓扑的发现；不需要输入或选择其他内容。发现过程监控会显示一下内容：

- ping 所有网络设备的进度
- 采集有关 SNMP 信息的进度
- 发现物理拓扑的信息
- 保存发现的拓扑结果



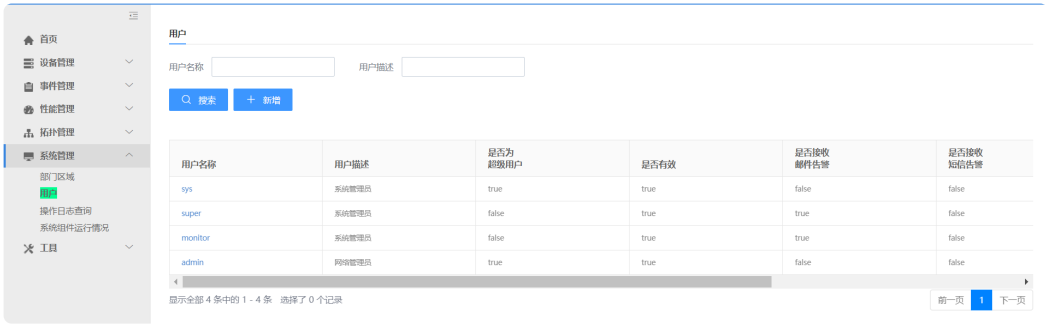
物理拓扑图

拓扑发现完毕后，可以看看整体拓扑情况。打开拓扑图后，首先手工调整拓扑图的布局，然后保存下来：



系统管理

系统管理主要维护用户（操作员）信息。系统采用单点登录方式登录蓝鲸 PaaS 平台，并可以重新定义普通用户的角色。



“部门区域管理”用于设备按部门区域进行分组管理。

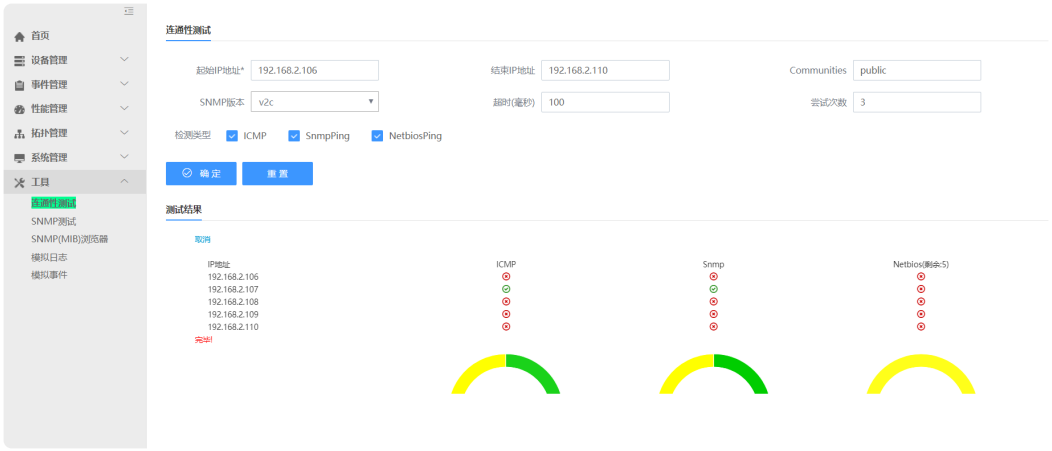
工具

系统提供了一下常见的工具：

- 连通性测试
- SNMP 测试
- MIB 浏览器
- 事件模拟

- 日志模拟

“连通性测试”主要通过 ICMP，SNMP 和 netbios 来测试网络设备和服务器的连通性，以及对 SNMP 的支持情况：



“SNMP 测试”是常用的工具，如果发现设备 SNMP 访问有问题或验证配置是否正确，应该使用该工具。

快速入门

登录蓝鲸平台后，在蓝鲸主页（Portal）中点击 “网络管理” 图标。

点击“网络管理主页”的上部“快速使用指南”连接

依照 4 个步骤完成系统的初次使用，包括：

确认系统各服务组件运行正常

“系统管理”----”系统组件运行情况”,出现下面 5 个组件的运行状态信息，确认红色框中的组件运行正常。

- Geneinfo:系统主程序
- Perfd：性能数据采集和处理程序
- Syslogd：Syslog 采集和处理程序
- CleadDatad：数据清理程序。缺省性能数据保存 90 天，严重的事件信息保存 1 年，一般的事件信息保存 90 天
- Discoveryd：设备自动扫描程序

开通设备的 SNMP 服务器和 Syslog 服务

所有纳管设备必须支持 ping（不能禁 ping）和 SNMP，网络设备同时要开通 Syslog 服务，Linux 系统可以将 syslog 转发到网络管理服务器。

- 网络管理员可以登录到网络设备上手工执行有关命令，以开通和设置 SNMP，Syslog 服务
- 也可以使用“开通 SNMP 和 Syslog”，采用 ssh 远程执行相关命令的方式，如下图所示:

如红色框中的命令可以是:

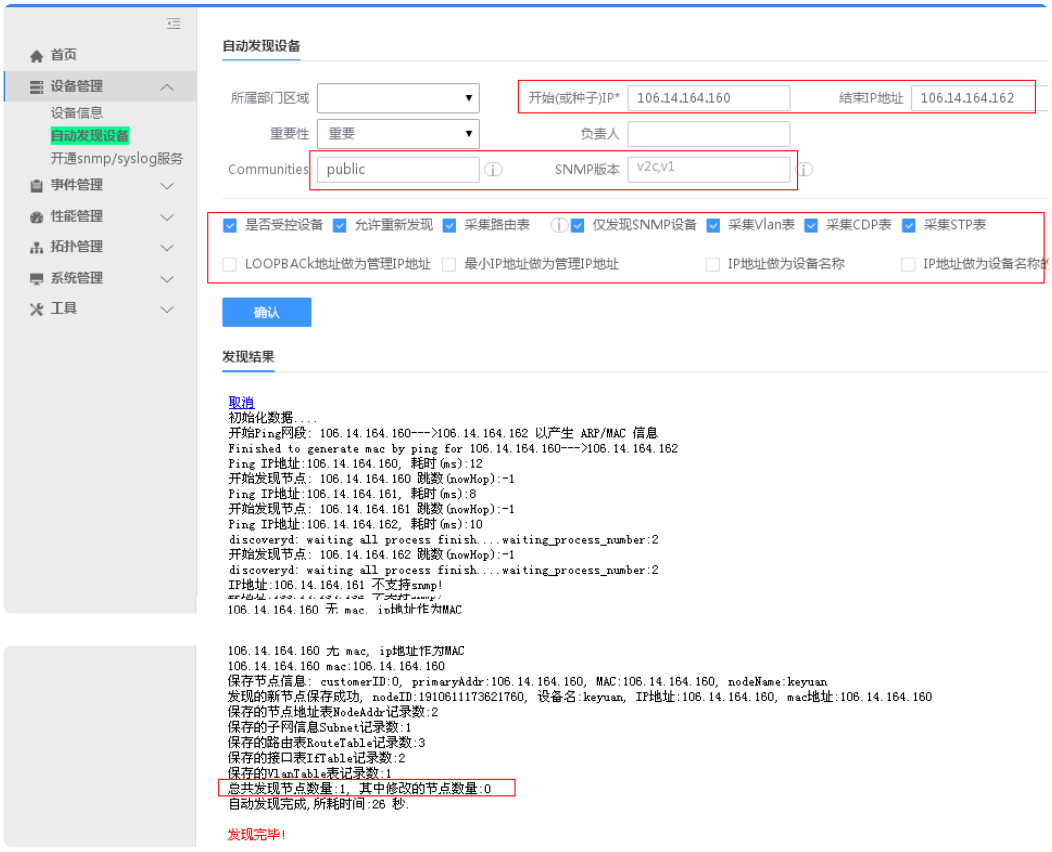
```
config
snmp-server community nmsread ro
logging on
logging 10.2.2.1
end
```

假设网管服务器的 IP 地址为 10.2.2.1； 假设设置 read community 为 nmsread

- Linux 和 Windows 的 SNMP 设置可参考系统的“开通 SNMP 和 Syslog” 功能页面中的说明

自动扫描发现设备及其模块

点击”设备管理”--”自动发现设备”，再界面中最小输入为：起始 IP 地址和 community。 一般输入一个 IP 地址段，设备的 community， SNMP 版本输入:v2, 其它选项不用改变。



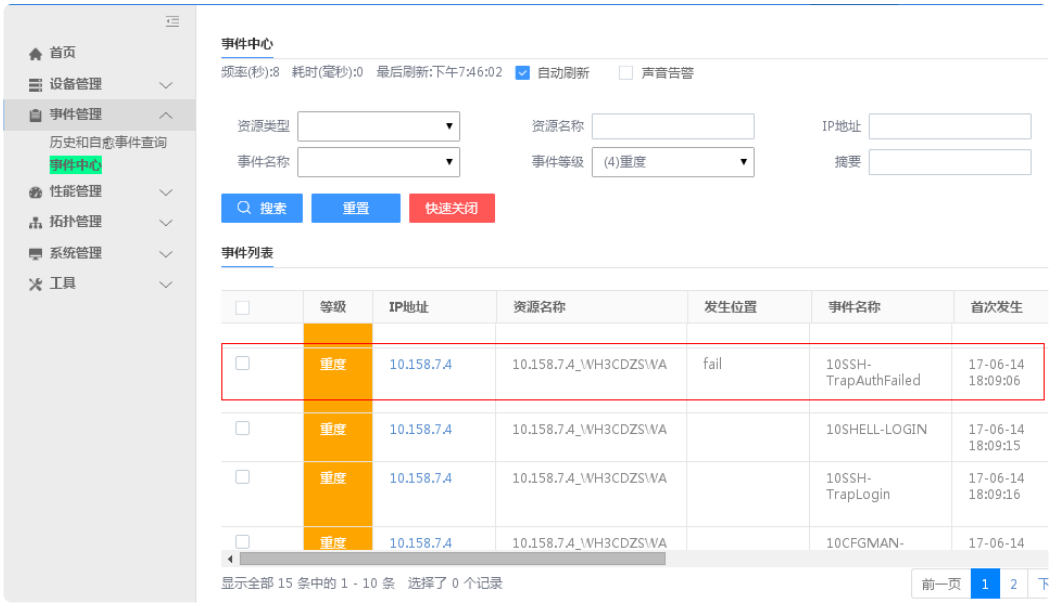
如上图所示，发现完毕后，会给出发现设备数量的统计信息，和保存了哪些设备信息。

再次强调：设备要能 ping 的通，并且支持 SNMP 才会自动发现出来。

自动接收 Syslog 信息和自动进行事件（故障）处理

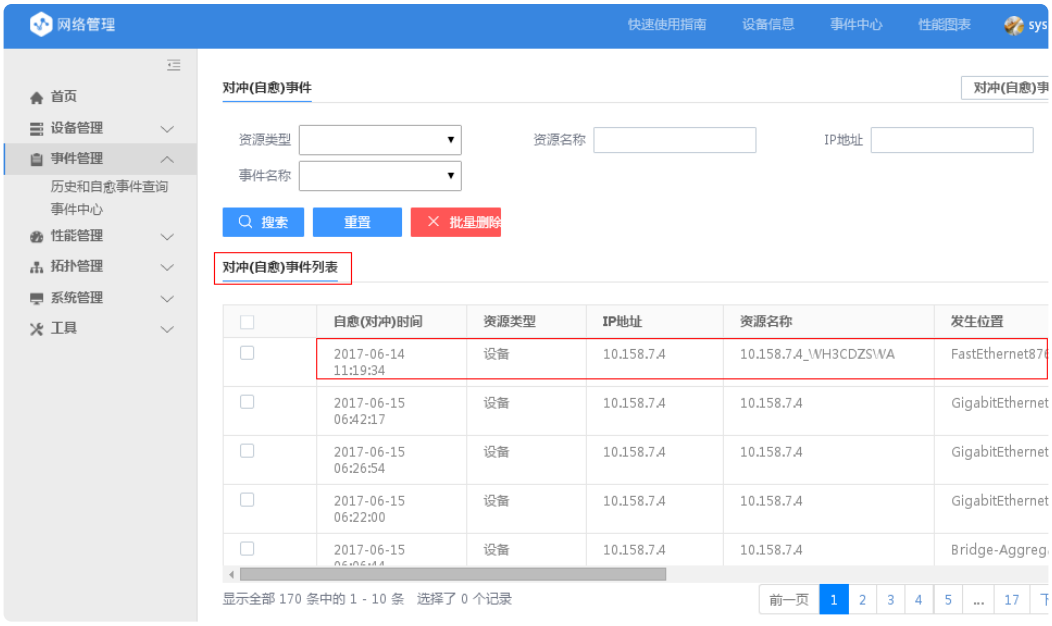
- 系统(Syslogd 服务组件)等待收集 Syslog 日志信息的服务端口为 UDP 514。
- 系统收到 Syslog 会根据内置的处理，进行抛弃，丰富，压缩，自愈，升降机，转发，关联，告警等处理。
- 处理后的事件首先保存到事件中心，然后保存到历史事件中，如下图所示：

首先保存到“事件中心“



然后保存到“历史事件“中：

如果发生了对冲（自愈）处理，则“抵消“后的事件信息，保存到”对冲（自愈）事件中。



新发现的设备等待 25 分钟左右，会自动采集（基础）性能数据

- 新发现的设备系统缺省 25 分钟左右会采集相应的性能数据：
  所有交换机和路由器设备会采集端口流量信息
  Cisco 和 H3C 设备会采集 CPU 和内存利用率
  Linux 和 Windows 服务器会采集 CPU，内存，磁盘和 Swap 利用率
- 设备新发现后，也可以点击“系统组件运行情况“中的 Perfd 的”刷新业务参数“，使系统立即采集设备的性能数据，如下图所示：

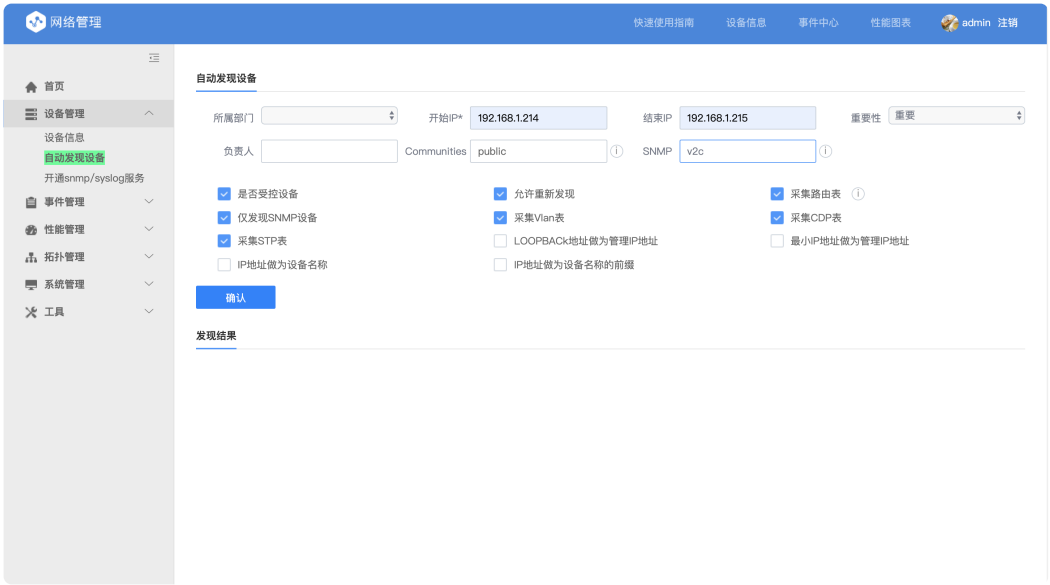
接收邮件或短信或微信告警（如果事件（故障）等级为最高级，即严重等级）

- 系统缺省将最高等级的事件（5 级：严重事件）发给能够接收告警信息的用户。
- 哪些用户能够接收告警信息，在“用户“管理界面中定义，如下图所示：

设备发现

在安装完网络设备管理后，如相关网络设备已配置 SNMP，可直接通过 **设备管理-自动发现设备** 功能进行设备的自动发现和入库。

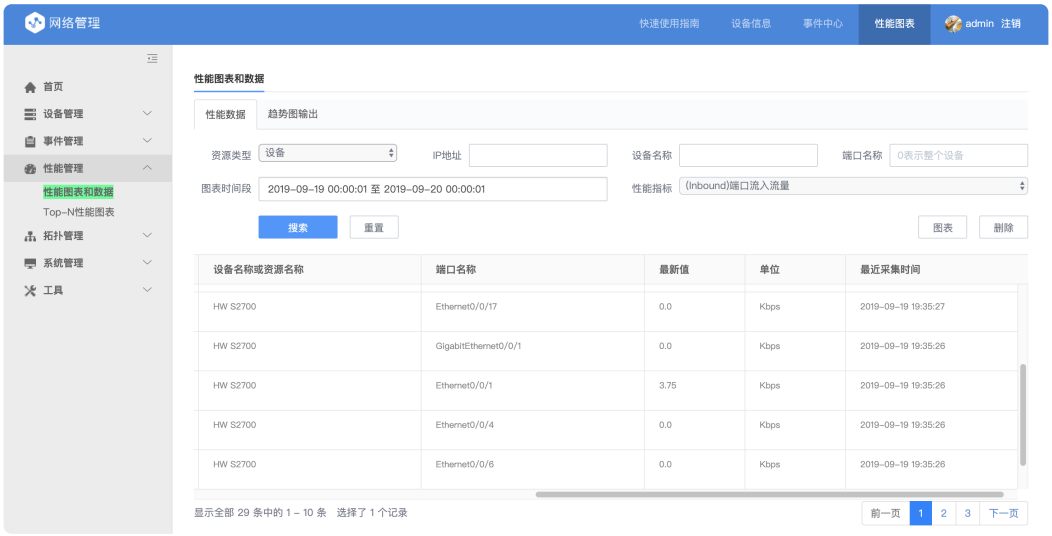
主要填写的配置内容为：开始 IP、结束 IP、Communities 和 SNMP 版本。



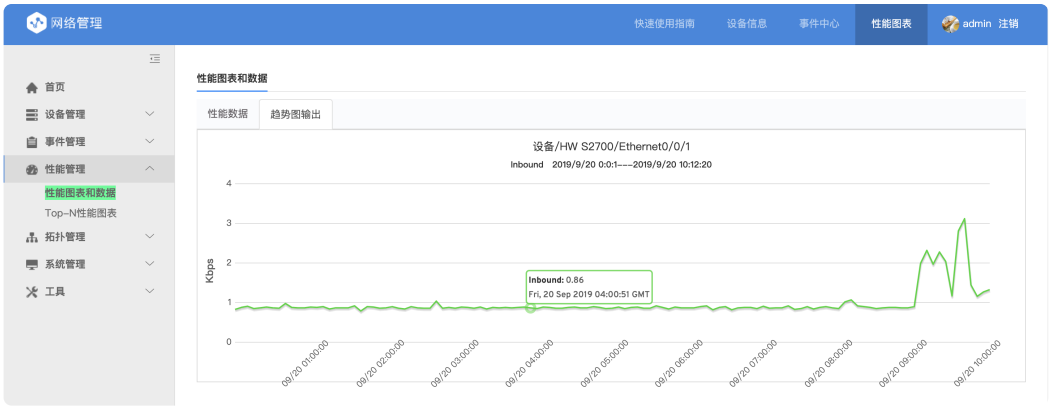
点击确认按钮后，网管即对网段进行 ICMP 扫描，扫描结果也会实施显示在下方信息栏

性能管理&事件管理

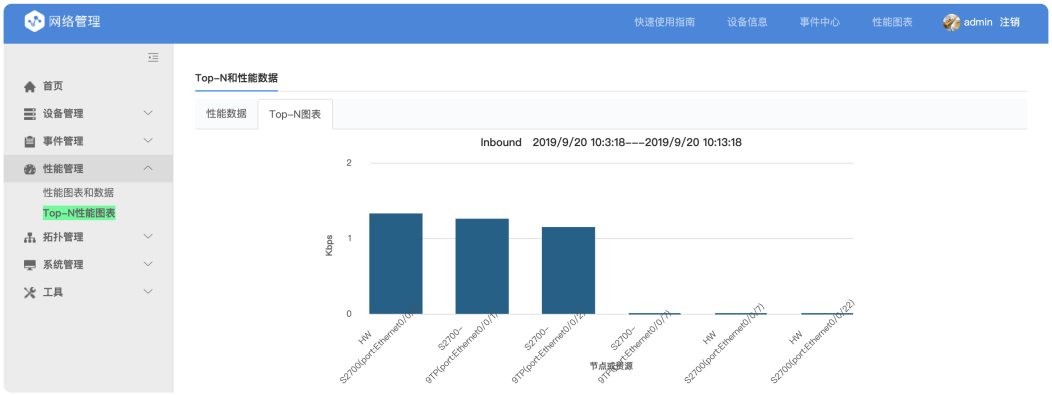
在设备发现完成后，网管平台自动对已发现的设备进行性能采集和事件接收。 进入 **性能管理-性能图表和数据** 可直接观察到最新的采集数据。



选择性能指标后，点击图表，即可观察设备的性能的图形化数据



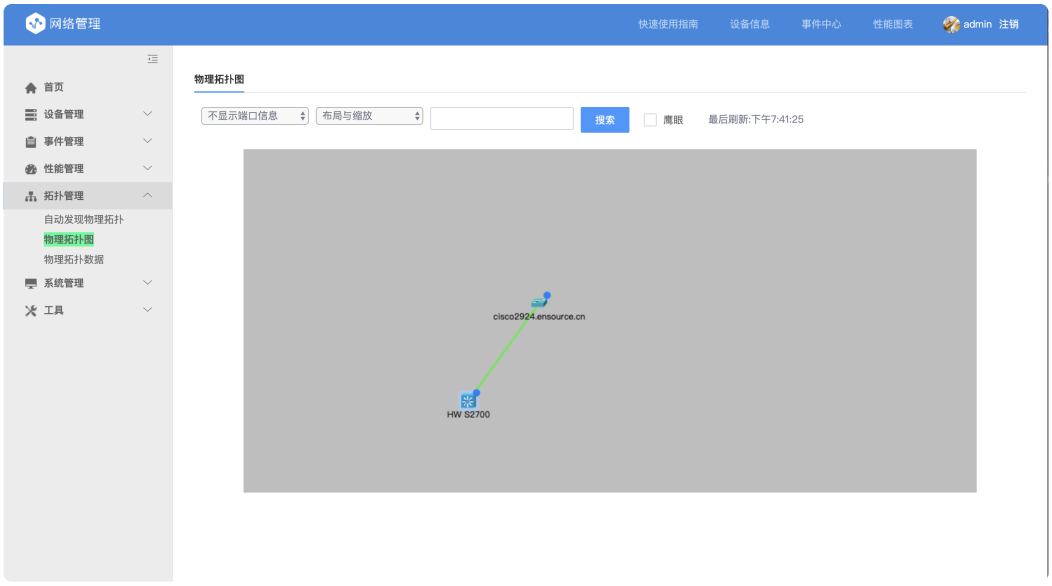
同理，TOPN 展示



拓扑

进入 **拓扑管理-自动发现物理拓扑** 点击确认，后台自动发现拓扑信息。

进入 **拓扑管理-物理拓扑图** 即可观察发现的拓扑图形



常见问题

如何开通设备的 snmp 和 syslog 服务

网络设备需要开通和设置好 snmp 和 syslog 服务，才能纳入监控管理。有 3 种情况：

- 请求网络管理员用手工方式开通和设置 Cisco，华为，H3C 等网络设备的 snmp 和 syslog 服务
- Linux 和 Windows 的 snmp 设置可参考系统的“开通 snmp 和 syslog” 功能页面中的说明
- 使用“开通 snmp 和 syslog”功能页面，采用 ssh 方式一台台开通设备的 snmp 和 syslog 服务

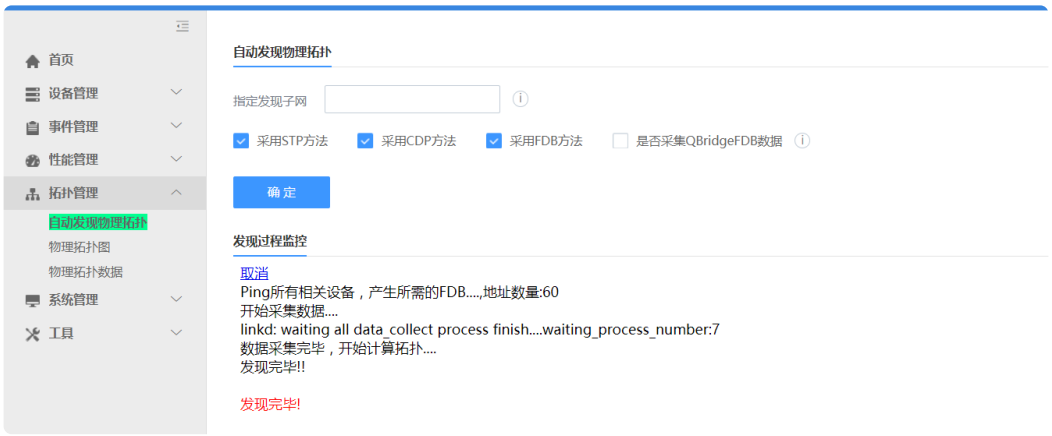
如何自动发现设备及其模块

首先设备要开通 snmp 服务。然后在“自动发现设备”页面中，输入起始 IP 地址和终止 IP 地址，点击“确认”，如下图所示。发现过程会提示本次新发现了多少设备，重新发现了多少设备。如果是重新发现的设备，可能会同时发现出设备名称的改变，也会做出提示，并生成一条事件信息。

发现完毕后，可以转到“设备信息”页面中查询新发现设备的详细信息。

如何自动发现物理拓扑和调整物理拓扑

系统采用了 CDP,STP 和 FDB 三种发现方式，以尽可能完整准确的发现异构网络环境的真实的物理拓扑结构。 选择“自动发现物理拓扑”菜单项，出现下面的页面：



然后**不要输入任何信息**，再直接点击“确认”，将显示发现过程，发现信息会提示本次发现的（新的或修改的）物理连接信息。发现完毕后，可转入“物理拓扑图”，查看物理拓扑。

没有进行拓扑图的发现前，物理拓扑图中显示的是散列的各个设备。

物理拓扑图初始是没有进行布局调整的界面，所以会显得比较零乱，此时需要进行手工调整布局，然后保存下来即可。

如何请求和使用其他应用功能

社区版提供了网络管理基本和实用的功能，能满足日常基本上的网络监控管理需要。而其他工作则需要升级到企业版或云版，它们提供了更为全面的功能，如：

- 统计报表
- 拓扑连接的手工可视化调整

- 客户化的 KPI 定义
- 客户化的阀值定义
- 流量管理
- 链路管理
- 专线管理
- 网络服务（ISM）管理
- 逻辑拓扑的自动发现
- 多租户支持