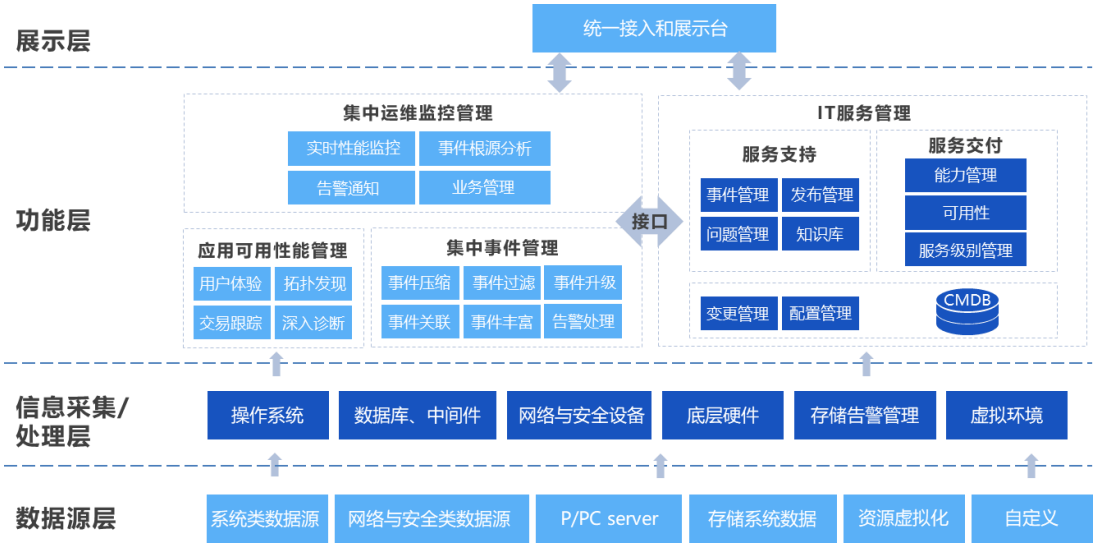
1.2 统一监控平台

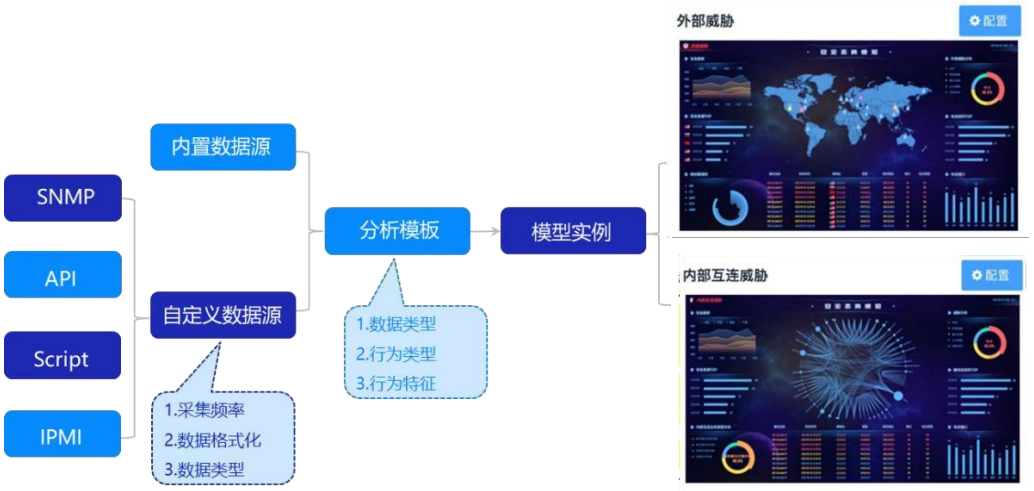
通过 SNMP、IPMI、PING、HTTP、SSH、Telnet、WMI、Agent 等多种技术协议和方式，实现对数据中心信息化资源环境中的网络设备、安全设备、主机设备、业务系统、机房环境等进行 7×24 小时监控，随时关注关键指标的健康度， 及时预判潜在的问题，如有发现异常自动告警，并通过短信、邮件多种方式通知到相关人员。通过对监控数据进行分析实时展示设备、网络、系统软件等的运行状态和业务健康度，并通过图表、拓扑图等形式进行展示，为运维人员提供直观、高效的决策依据。

系统监测指标可覆盖用户 90%的需求，监测指标历史数据可保存 180 天以上，并可自行设置各指标的告警阈值。

监控架构设计图：



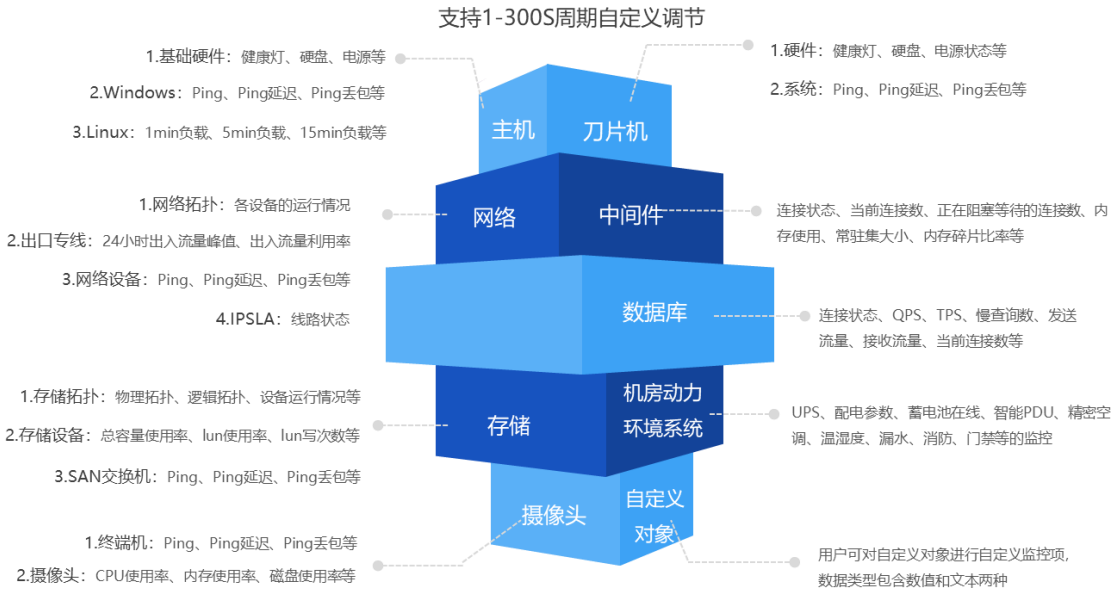
1.2.1 监控数据源管理



微梦云监控功能模块的数据源包含内置数据源与自定义数据源，内置数据源是指系统内置各类对象常规监控项及其数据来源方式（如SNMP、SSH、TelnetWMI等数据采集方式）自定义数据源是指在内置监控项不满足监控需求时，用户可能通过 SNMP、API、Script、IPMI 等方式自定义数据源，从而完成自定义相关监控项。

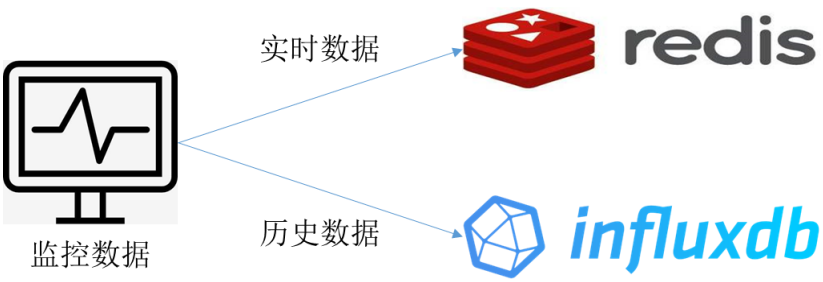
将所有运维系统的数据整合之后，告警实现采用内置数据源、自定义数据源、数据模板来实现不同数据的告警通知。

1.2.2 监控项设计



如上图所示，系统内置多种模型及其监控项，内置监控项通过自研 Agent、SNMP、IPMI、WMI、SSH、脚本、第三方上传等多种方式进行采集监控数据。除了内置监控项外，用户还可以自身的监控需求进行自定义监控项。

1.2.3 监控数据存储



微梦云监控平台中的数据分为实时数据与历史数据，实时数据存储于 Redis， 历史数据存储于 Influxdb。由于监控数据是需要进行实时采集，数据量巨大，所

以采用此结构可以快速的进行监控数据处理与展示。

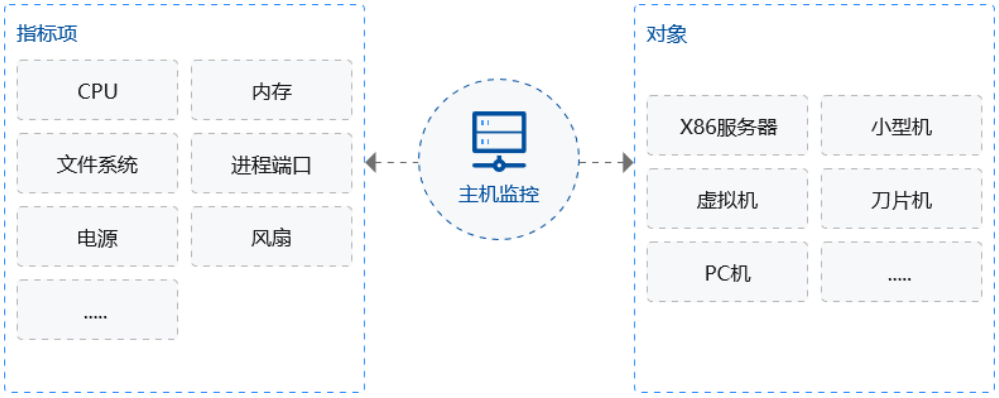
1.2.4 主机监控

对于主机的监控管理，本系统支持通过 SNMP 协议、自研 Agent 程序、IPM I 协议、SSH 协议等方式进行采集监控数据。

1、支持多类型主机设备接入：市面上主流的云主机（腾讯云、阿里云、华为云、Azure 等主流云厂家）本地主机均可接入至微梦云运维平台进行统一监管， 支持 Windows、Linux、Unix 等主流操作系统。

2、拥有专业的主机设备性能监控：云主机支持通过云厂家提供的监控 API 进行对接（无需安装 Agent），而本地主机支持通过 Agent 监控系统性能状态，通过IPMI 协议监控设备硬件性能状态；拥有二十多项性能监控指标，如 CPU、内存、磁盘容量、磁盘 IO、进程、TCP 连接数、网口流量、温度、功率等性能监控指标。

3、监控实时性强、数据保存时间长：监控数据可达到秒级，出现故障可及时告警，减少故障发现时差；监控数据至 少可保存 180 天，满足等保、网络安全法等法规。



1.2.5 虚拟化监控

支持对主流虚拟化平台的监控管理，如 VMware、华为、华三、深信服等虚拟化平台。系统通过虚拟化平台有权限采集数据的账号即可将虚拟化平台的数据采集到监控平台中。支持采集虚拟化平台中的宿主主机数量、虚拟机数据、宿主机基础性能数据、虚拟机基础性能数据、网络端口情况、虚拟化平台中存储容量情况等内容，并支持自定义监控项。

微梦云监控平台支持采用无代理或代理方式对虚拟化平台中的虚拟机进行采

集监控数据，通过自研 Agent 可以获取到虚拟机操作系统层面更详细的监控数据，如 CPU 利用率、内存利用率、磁盘利用率、磁盘 I/O、连接数、进程、端口流量等详细内容。

通过采集虚拟化平台的网络数据，还可以自动生成虚拟化平台虚拟机之间网络拓扑图。

1.2.6 网络监控

对企业网络环境进行实时监控，并获取网络最新运行情况，实现对网络环境中的网络/安全设备、线路等进行运行状态展示、故障发现、故障预警、故障定位等一体化综合监控，最终保证网络系统持续、稳定、安全运行。

对于网络/安全设备采用 SNMP 协议进行采集相关监控信息（如设备名称、端口数量、端口速率、端口状态、端口出入流量、端口错包率、端口丢包率、电源状态、CPU 利用率、内存利用率、磁盘利用率等）

1.2.7 存储监控

支持通过 SNMP 协议采集存储的监控数据。存储设备监控支持的品牌包含 IBM、NetApp 等主流厂商，同时支持监控博科 SAN 交换机。

存储系统监控内容包含：硬件状态（如电源、风扇等）连接状态、设备状态、磁盘监控（如总容量使用率、磁盘活动数、磁盘总写入、磁盘总读取、磁盘故障数）LUN 监控（如LUN 使用率、LUN 写次数、LUN 读次数等）互联主机数、FC 端口状态变化、FC 端口出入流量、FC 端口出入吞吐量、互联信息等。

SAN 交换机监控指标包含：设备状态、电源状态、连接状态、健康状况、端口使用状况、互联信息、Ping 延迟、Ping 丢包、端口入流量、端口出流量、端口

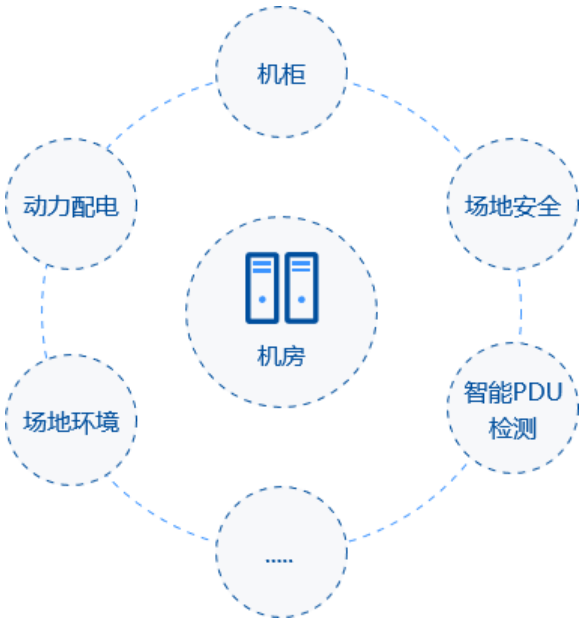
入吞吐量、端口出吞吐量、端口错误数、互联主机数等。

支持以拓扑图的方式展现存储与服务器之间的连接关系、LUN 与存储之间的连接关系。

支持查询存储与 SAN 交换机所有指标的历史监控数据，关键指标（如总容量使用率、LUN 使用率、LUN 写次数、LUN 读次数、出流量、入流量、磁盘活动数、磁盘故障数、磁盘总读取、磁盘总写入、互联主机数、Ping 延迟、Ping 丢包等）能以折线图展示。

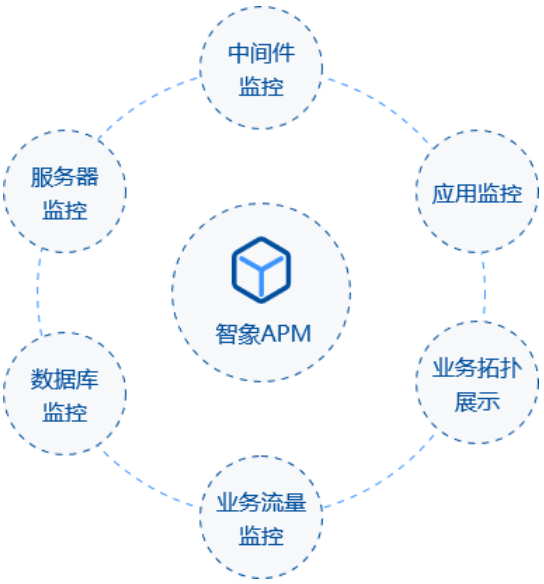
1.2.8 IDC（机房）监控

IDC 机房监控主要围绕机房动力环境（动力配电、场地安全、场地环境等）机柜容量、PDU 使用情况等多方面进行全方位监控，以及机房设备资产管理，实现IT 基础设施与机房动力环境一体化监控管理，从而使 IDC 机房以高质量、精细化运维与运营。



1.2.9 APM 监控

非侵入式的应用监控，支持标准应用、数据库、中间件、网站、Web 服务等， 并可自定义应用内部监测指标，借助直观的视图，轻松洞悉复杂 IT 环境中的各组件之间的关系，快速定位故障根源。系统提供了业务建模工具，可以构建业务拓扑，以此构建业务健康指标体系，从业务的性能与可用性和业务的威胁维度计算业务的健康度。用户可以对业务进行可用性分析，查看业务监控事件和业务告警，用户可以对业务拓扑进行钻取，分析构成业务的每个资产的运行详情。



微梦云 APM 内置监控对象如下：

- 中间件监控：Redis、WebLogic、WebSphere、Tomcat、Nginx 等；
- 数据库监控：Mysql、SQL Server、Oracle、Sybase、DB2、MongoDB 等；
- 标准应用监控：Apache、IIS、Exchange、Postfix、AD 域控等；
- 自定义监控：支持用户通过脚本、第三方接口等方式监控自定义应用。

1.2.10 U 位监控

通过为设备分配的电子标签，结合智能 U 位装置，实时检测上报设备所在的机柜和 U 位，发现位置异常自动报警。实现了 U 位与设备关系的精确化管理， 避免因位置不准确而导致的资产丢失、运营事故。

1.2.11 拓扑监控

自动生成网络拓扑，智能发现网络回环、多链路，可自行过滤、选择、拖拽生成所需的拓扑结构，同时可在网络拓扑图上显示相关设备、网络连接的静态信息和动态指标，如有异常，也可直接在拓扑图上显示并进行告警通知。

1.2.12 配置监控

支持监测网络设备配置的变更情况，如有变更则通知相关运维人员；同时支持安全配置基线核查管理，通过对目标系统展开合规安全检查，找出不符合的项并选择实施安全措施来控制安全风险。

1.2.13 大屏监控

将监控数据、指标以 2/3D 图、表、动画等形式在大屏幕上直观的显示出来，

方便运维人员实时查看设备（系统）状态，满足精细化业务需求。大屏显示提供个性化定制服务。

1.2.14 自定义监控项

自定义监控支持自定义监控项和自定义布局展示。采用全自定义方式实现对设备动态信息、状态信息、静态信息进行采集、格式化、存储、展示。自定义使用户可轻松扩容监控指标，实现对设备的全覆盖监控。自定义监控项支持通过 SNMP、脚本、第三方上传等方式进行自定义监控数据采集。

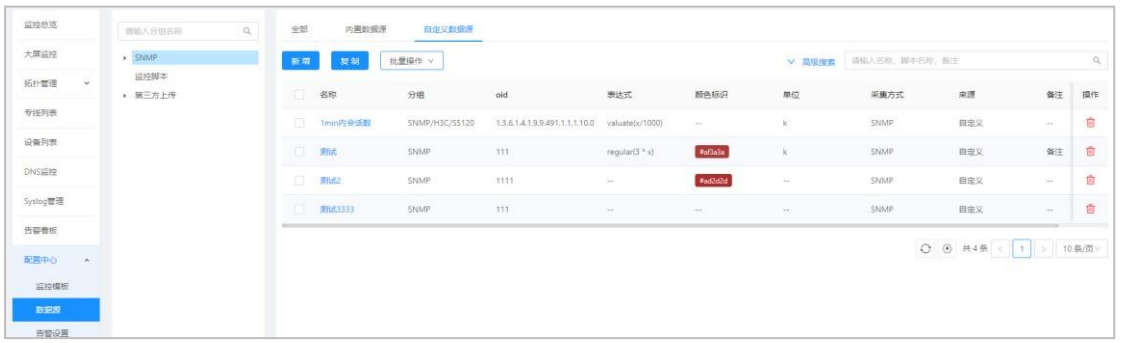


图-自定义监控项

图-自定义布局展示

1.2.15 告警管理

告警依赖于监控提供的数据信息，统一监控平台实现告警信息的分级、过滤、阈值定义，并提供集中统一的界面，对实时、预警、历史告警信息进行展示和管理。

功能包含：告警信息、告警级别、告警显示、告警过滤、告警策略、告警阈值。

4.2.12.1 告警管理架构

数据模板是指对象监控采集项来源，定时（可自定义采集间隔）采集监控对象的具体监控指标。数据模板匹配模板化告警规则，实现对告警的级别、类型、通知人员、恢复机制、阶梯等不同维度的展示。

支持通过短信、邮件、微信、钉钉、系统等方式进行告警通知。

4.2.12.2 告警信息

告警信息分为实时告警信息和历史告警信息；

实时告警信息包括：告警源、告警类型、告警级别、告警内容、告警原因、告警发生时间；

历史告警信息包括：告警源、告警类型、告警级别、告警内容、告警原因、告警发生时间、告警结束时间、告警确认时间、告警确认人。

4.2.12.3 告警级别

1、告警级别默认为三级，分为普通、一般、严重，可自定义；

2、根据告警级别设置不同显示颜色，方便运维人员通过颜色就能一眼识别出告警的级别，使运维人员快速找告警级别高的事件，从而提升故障解决效率；

3、用户可以根据自身业务特点进行自定义告警级别。

4.2.12.4 告警显示

1、告警以列表方式展现，根据告警级别显示不同颜色；

2、可以根据告警级别排序；

3、告警信息根据权限过滤；

4、告警显示页面定时自动刷新；

5、有新告警信息时，页面可以发出告警声音；

6、显示告警的详细信息和告警通知情况。

4.2.12.5 告警过滤

1、支持告警过滤功能，可根据用户设定的显示过滤条件，有选择地显示当前告警事件；

2、支持正则表达式的告警信息过滤功能，并根据需要保存成告警类别；

3、过滤条件包括告警源、告警级别、告警类型、告警状态、告警内容等组合（逻辑与、逻辑或等）来设定；可对日常设备维护期内出现的大量告警事件进行过滤。

4.2.12.6 告警收敛

告警面临最大的问题就是警报太多，造成“告警风暴”，运维人员将会不断的接受到告警通知，相当于“狼来了”的形式，收件人会对收到的这些告警信息感到麻木，还会造成关键的告警被淹没，对运维人员造成了困扰，也给排查问题带了不小的难度。

为了解决上述问题，根据定义好的一系列收敛规则（支持设置收敛频率、收敛上限、收敛时间等），对告警进行归类压缩、分析或直接丢弃，将同类告警聚合，当报警发出后，则停止重复发送由此告警引发的其它告警，从而降低误报率，减少报警信息，避免“告警风暴”的发生。

4.2.12.7 告警策略

告警监测到的所有事件应形成告警记录，并按照预先设置的告警策略通知运维人员处理。

1、具备短信、邮件、系统、微信、钉钉等告警通知方式，告警方式可灵活组合，告警策略可设置有效时间；

2、支持告警动作模式灵活组合功能，实现不同时段执行不同的告警策略；

3、具备告警策略延时功能，告警如在延时判断期内恢复，系统只形成告警记录，不执行告警动作策略；

4、支持告警确认功能，用户可手工进行告警确认，同时记录手动确认者的身份、确认时间等；

5、提供机制保存和积累处理告警的专家建议，并形成知识库。

4.2.12.8 告警阈值

告警阈值设置支持手工告警阈值设置和系统智能阈值自动设置。

★ 手工设置告警阈值

对于告警规则设置，提供性能阈值规则的维护界面。另外，系统提供的告警内容能比较全面地描述该性能数据超出阈值的情况，方便分析、排除故障。监测阈值规则的设置具备以下功能：

1、能针对不同告警级别、监测对象的性能指标，定义不同的阈值；

2、设置监测阈值时可以设置为：范围之内、范围之外、变化大于、变化小于等阈值策略。

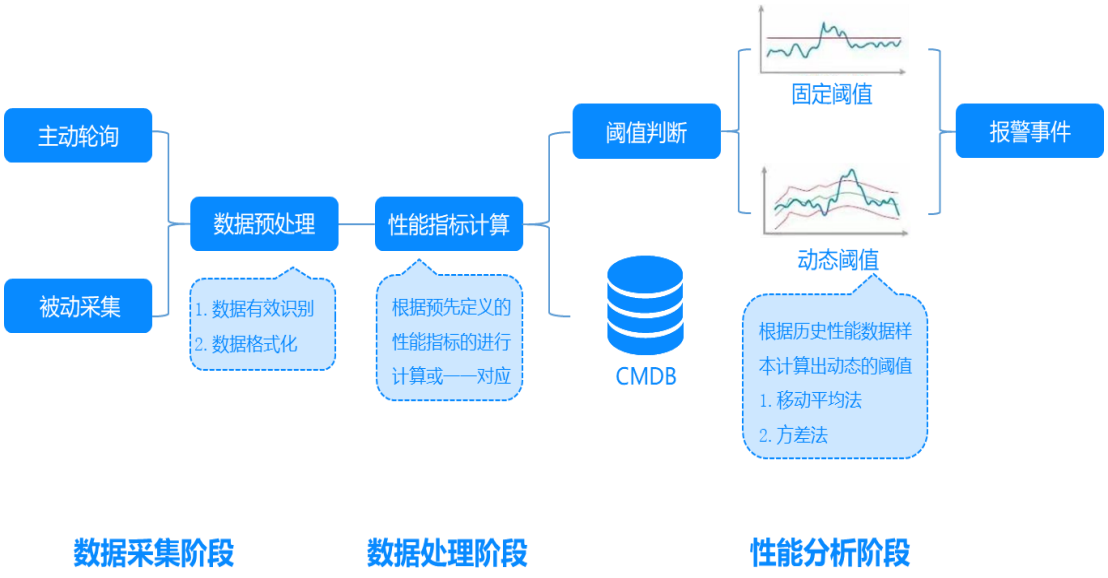
3、支持批量修改阈值，无数量限制；

4、监测轮询采集数据间隔最小 15 秒；

★ 智能阈值

基本动态学习的智能阈值告警，可降低告警错报率，及时预判潜在的问题，如有发现异常自动告警，并通过短信、微信、邮件、钉钉多种方式通知到相关人员。

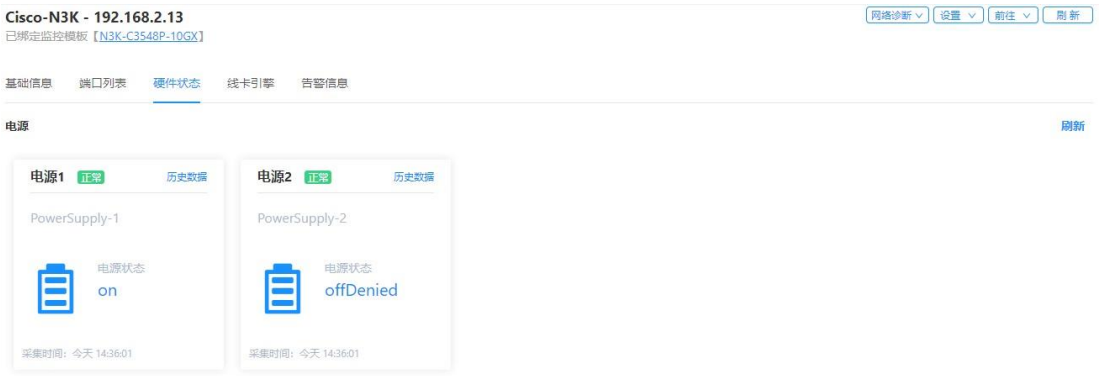
智能阈值处理流程图如下所示：



1.2.16 部分界面展示


Cisco-N3K - 192.168.2.13
已绑定监控模板【N3K-C3548P-10GX】
基础信息
端口列表
硬件状态
线卡引擎
告警信息
资源属性
思科
主机名： Cisco-N3K
IP： 192.168.2.13
资产编号： SW-2020-0207-004
设备型号： N3K-C3548P-10GX
设备序列号： FOC2027R07K
设备状态： 运营中
设备角色： --
业务区： --
负责人： --
设备高度： 1
设备位置： 智象科技/A004 (第40U)
备注： --
未知： --


图形展示
CPU使用率 正常 历史数据
3 %
采集时间：今天 14:35:01
内存使用率 正常 历史数据
64 %
采集时间：今天 14:35:01
设备运行时长 正常 历史数据
3天5小时12分钟
31秒
采集时间：今天 14:35:01


Cisco-N3K - 192.168.2.13
已绑定监控模板【N3K-C3548P-10GX】
网络诊断
设置
前往
刷新
基础信息
端口列表
硬件状态
线卡引擎
告警信息
电源
刷新
电源1 正常 历史数据
PowerSupply-1
电源状态
on
采集时间：今天 14:36:01
电源2 正常 历史数据
PowerSupply-2
电源状态
offDenied
采集时间：今天 14:36:01


风扇
风扇1 正常 历史数据
FanModule-1
风扇状态
up
采集时间：今天 14:36:01
风扇2 正常 历史数据
FanModule-2
风扇状态
up
采集时间：今天 14:36:01
风扇3 正常 历史数据
FanModule-3
风扇状态
up
采集时间：今天 14:36:01
风扇4 正常 历史数据
FanModule-4
风扇状态
up
采集时间：今天 14:36:02

智象-TO-东莞-01 机房专线 线路编号：ZX-DG-01 运营商：自有

监控概览 专线任务 流量视图 告警看板

属性资源 刷新

线路名称：智象-TO-东莞-01　　带宽：10 M　　本端设备端口：Cisco-4506-CoreSW: Gi4/5

对端设备端口：WorkSW03: GigabitEthernet1/0/23　　本端机房：智象科技　　对端机房：东莞机房

负责人：bingwei　　备注：--

监控概览 刷新

Cisco-4506-CoreSW
192.168.1.1

WorkSW03
192.168.2.3

配置概览 备份记录 恢复记录

基本信息 前往

思科

模型：交换机　　状态：正常

主机名: Cisco-N5K　　资产编号：SW-2020-0207-006

IP: 192.168.2.15　　备份任务：周期备份

配置信息 设置 配置拉取 过滤规则：启用

运行配置 下载 复制

```
version 5.2(1)N1(4)
logging level feature-mgr 0
hostname Cisco-N5K
feature telnet
feature lacp
feature lldp
feature fex
username admin password 5 $1$oZcUpUFG$nj6hLOb6niyYCgXxym7vZ/  role network-
no password strength-check
banner motd #Nexus 5000 Switch
#
ip domain-lookup
class-map type qos class-fcoe
class-map type queuing class-fcoe
  match qos-group 1
class-map type queuing class-all-flood
  match qos-group 2
class-map type queuing class-ip-multicast
  match qos-group 2
class-map type network-qos class-fcoe
```

启动配置 下载 复制

```
version 5.2(1)N1(4)
logging level feature-mgr 0
hostname Cisco-N5K
feature telnet
feature lacp
feature lldp
feature fex
username admin password 5 $1$oZcUpUFG$nj6hLOb6niyYCgXxym7vZ/  role network-
no password strength-check
banner motd #Nexus 5000 Switch
#
ip domain-lookup
class-map type qos class-fcoe
class-map type queuing class-fcoe
  match qos-group 1
class-map type queuing class-all-flood
  match qos-group 2
class-map type queuing class-ip-multicast
  match qos-group 2
class-map type network-qos class-fcoe
```