监控系统头脑风暴

编写人：王耀亨

2019-09-17

堡塔监控屏幕

网络数据

144s

浏览量(PV)	访客数(UV)	IP数
428,472	63,407	65,193

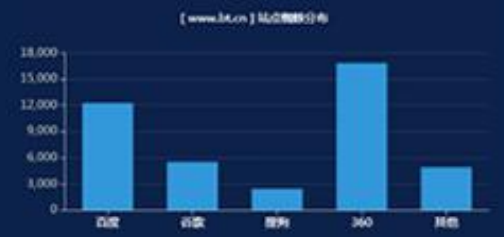
站点	PV	UV	IP数
www.bt.cn	378,500	48,926	46,931
[redacted]	2,399	66	1,668
[redacted]	1,150	145	839
[redacted]	1,053	29	512
download.bt.cn	337	23	185

蜘蛛分布

144s

百度	谷歌	搜狗	360	其他
30,734	5,532	4,910	33,673	4,953

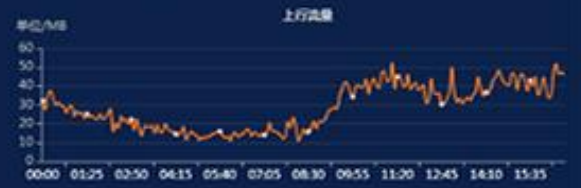
站点	百度	谷歌	搜狗	360	其他
www.bt.cn	12,257	5,526	2,463	16,819	4,918
docs.bt.cn	25	6	0	0	28
download.bt.cn	13	0	2	1	0
1[redacted]	0	0	0	0	0
[redacted]	0	0	0	0	5

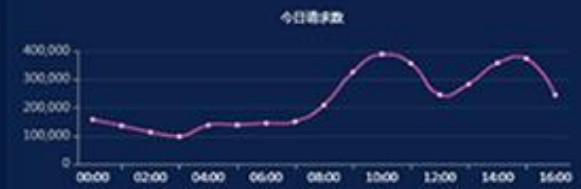


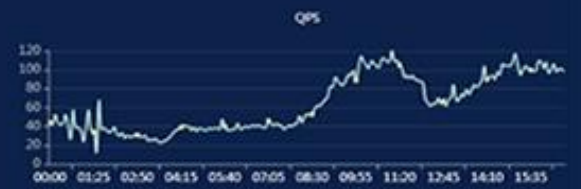
平台负载

144s

总负载	上行流量	今日请求数	QPS
10.16%	19.29 MB/s	3,868,625	106







单机状态

144s

IP	状态	负载	CPU	上行	下行	健康值
192.168.1.53	在线	0%	0.72%	240 B/s	7.04 KB/s	100
192.168.1.245	离线	0%	0%	0 B/s	0 B/s	90
192.168.1.1	在线	4%	5.69%	4.65 KB/s	1.17 KB/s	100
192.168.2.3	在线	0.5%	2.4%	394.55 KB/s	39.84 KB/s	100
192.168.3.1	在线	6.87%	23.91%	1.02 MB/s	286.15 KB/s	100

安全警告

144s

攻击	暴破
252,139	137

基线检测

144s

【2019/07/15 00:10:18】：192.168.1.123 3306 端口对外开放
【2019/07/15 00:10:18】：192.168.1.123 禁止SSH空密码用户登陆
【2019/07/15 00:10:18】：192.168.1.123 确保SSH LogLevel 设置为INFO
【2019/07/15 00:10:18】：192.168.1.123 设置SSH空闲超时退出时间
【2019/07/15 00:10:18】：192.168.1.123 SSHD 强制使用V2安全协议
【2019/07/15 00:10:18】：192.168.1.123 确保SSH MaxAuthTries 设置为3-6之间

登记记录

144s

【192.168.1.123】登录成功，账号：userxdc，登录IP：192.168.1.123

异常

144s

401	500	502	503
2	32	4,552	0

数据库慢查询	数据库连接上限次数	PHP慢日志数量	PHP并发上限次数
58	0	0	1

第一部分

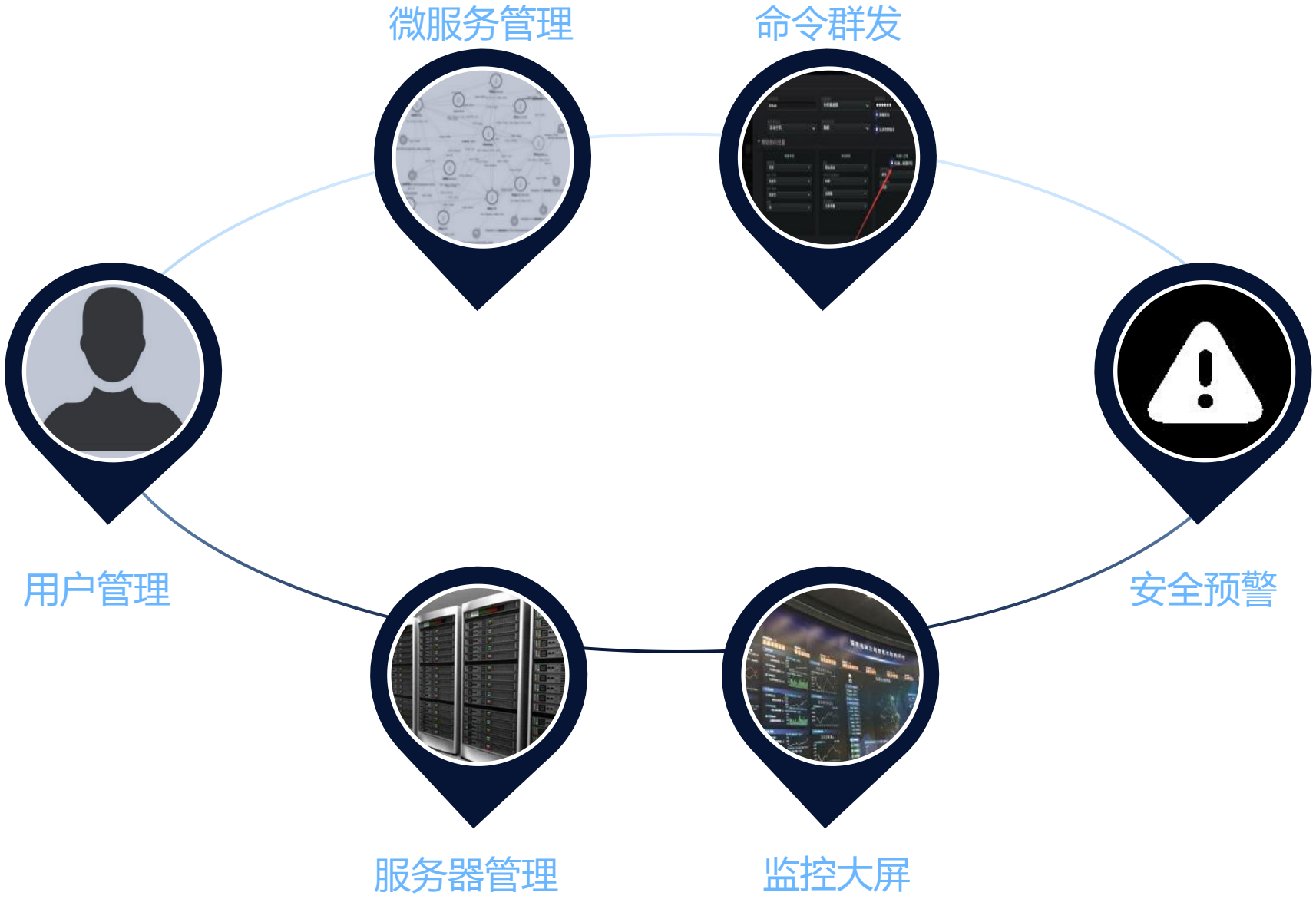
监控理论体系

自动化运维

自动化监控


监控评估
数据采集（主动）
Client
公共插件
自定义脚本
服务状态探测（被动）
服务状态
程序状态
用户访问质量
第三方信息
公司内相关系统
数据处理
复杂计算
阈值判断
智能分析
报警与联动
报警策略
联动处理
报警跟踪
问题管理
API

系统功能



监控对象分层

系统层

系统层主要是指CPU、磁盘、内存、网络等服务器层面的监控，这些一般也是运维人员比较关注的对象；

应用层

应用层指的是服务角度的监控，比如接口、框架、某个服务的健康状态等，一般是服务开发或框架开发人员关注的对象；

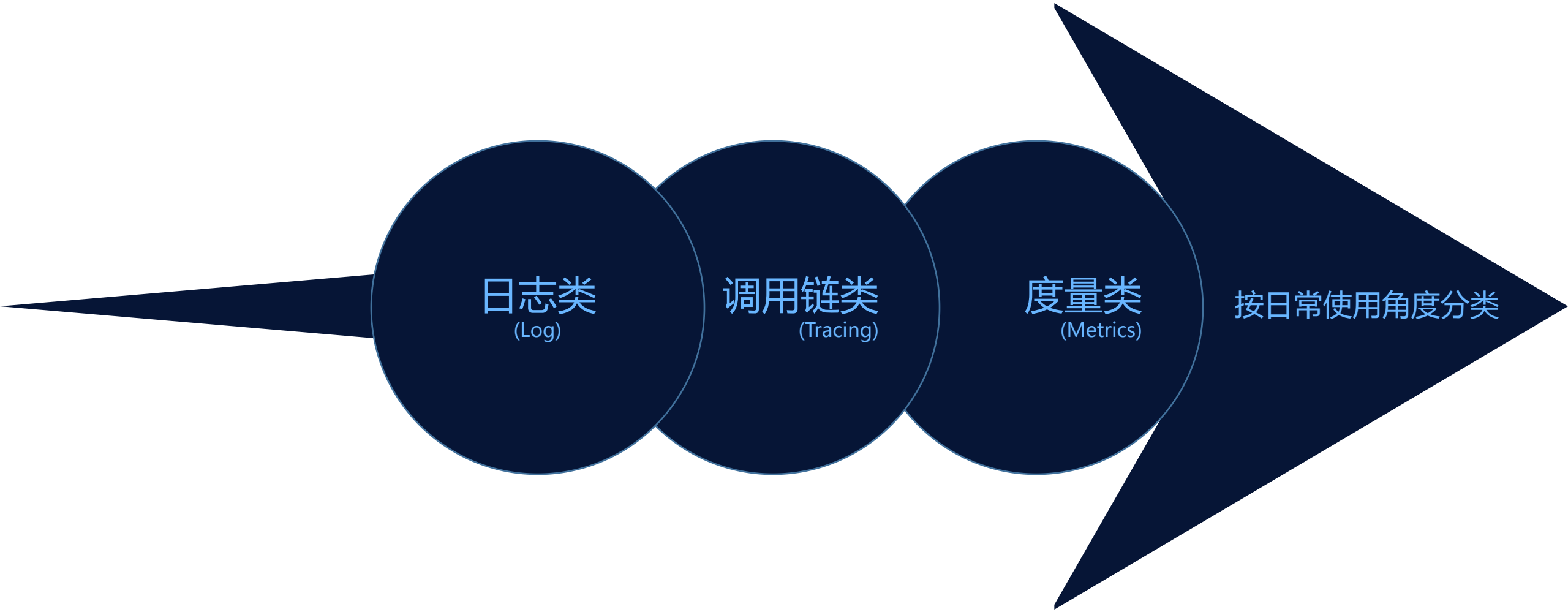
用户层

用户层主要是与用户、与业务相关的一些监控，属于功能层面的，大多数是项目经理或产品经理会比较关注的对象。

监控指标

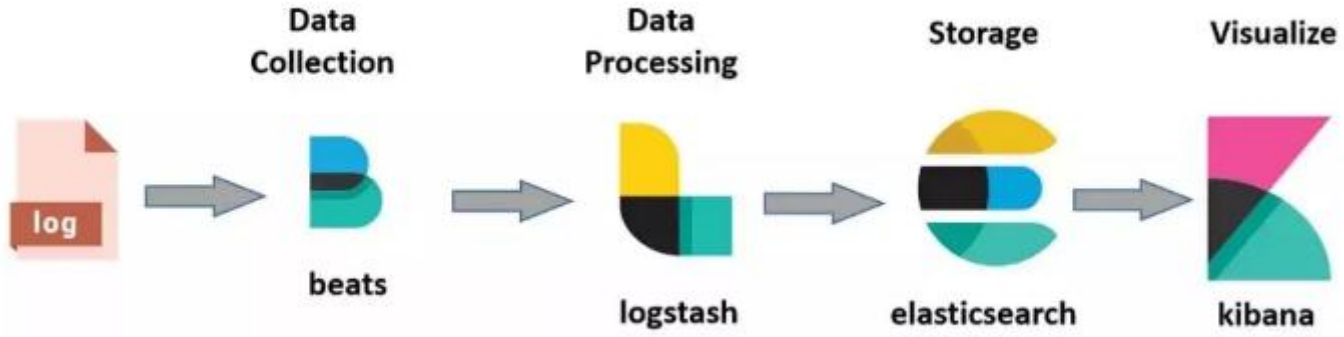
- **延迟时间**：主要是响应一个请求所消耗的延迟，比如某接口的HTTP请求平均响应时间为100ms；
- **请求量**：是指系统的容量吞吐能力，例如每秒处理多少次请求（QPS）作为指标；
- **错误率**：主要是用来监控错误发生的比例，比如将某接口一段时间内调用时失败的比例作为指标。

监控模式分类



日志类

1.日志类比较常见，我们的框架代码、系统环境，以及业务逻辑中一般都会产出一些日志，这些日志我们通常把它记录后统一收集起来，方便在需要的时候进行查询。日志类记录的信息一般是一些事件、非结构化的一些文本内容。日志的输出和处理的解决方案比较多，大家熟知的有ELK Stack方案（Elasticseach + Logstash + Kibana），如图：



调用链类

2.调用链类监控主要是指记录一个请求的全部流程。一个请求从开始进入，在微服务中调用不同的服务节点后，再返回给客户端，在这个过程中通过调用链参数来追寻全链路行为。通过这个方式可以很方便的知道请求在哪个环节出了故障，系统的瓶颈在哪儿。

这一类的监控一般采用CAT工具 来完成，一般在大中型项目较多用到，因为搭建起来有一定的成本。

度量类

3.度量类主要采用时序数据库的解决方案。它是以事件发生时间以及当前数值的角度来记录的监控信息，是可以聚合运算的，用于查看一些指标数据和指标趋势。所以这类监控主要不是用来查问题的，主要是用来看趋势的。

Metrics一般有5种基本的度量类型：

- Gauges（度量）；
- Counters（计数器）；
- Histograms（直方图）；
- Meters（TPS计算器）；
- Timers（计时器）。

报警系统

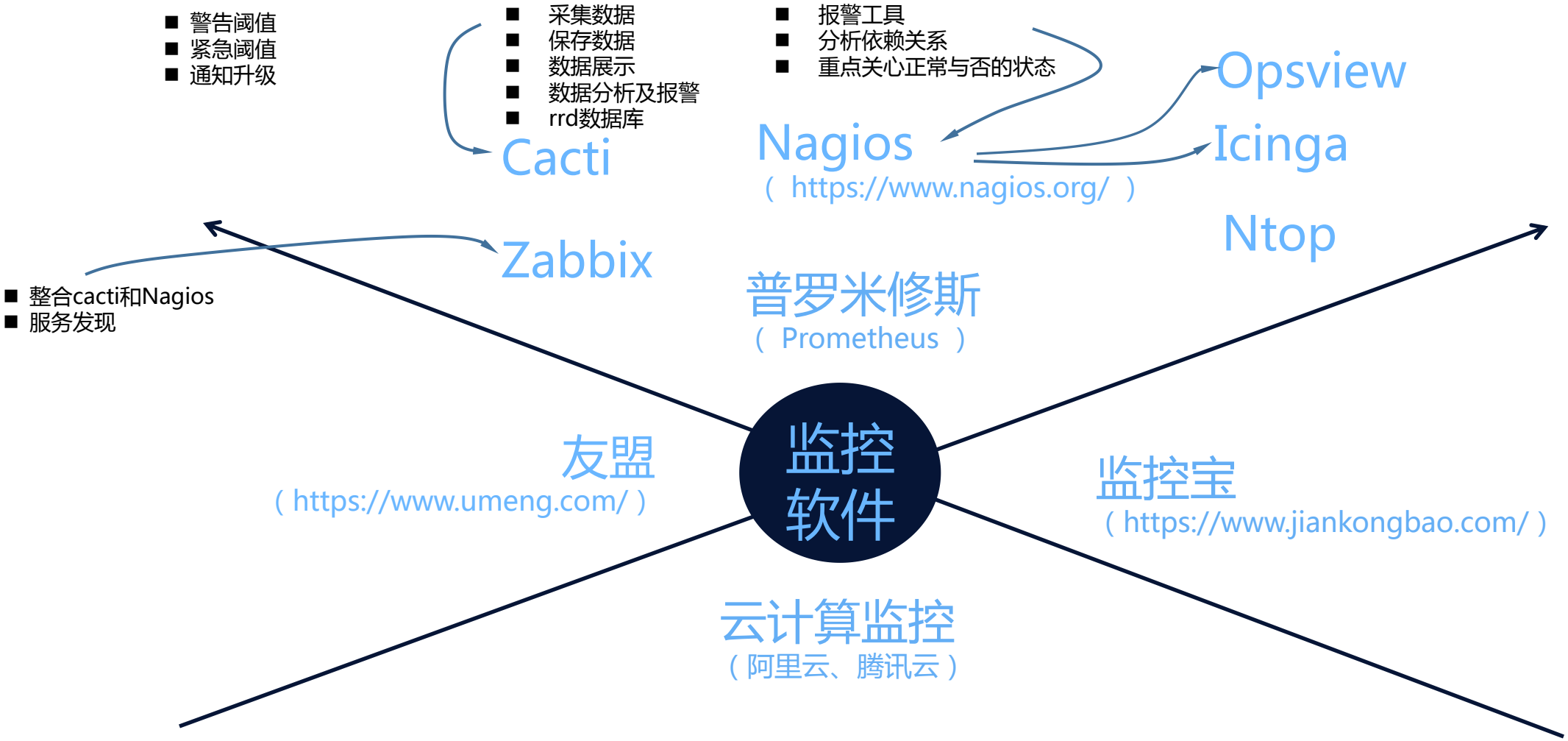
采集方式

- 后台式采集
- 一次性采集
- 桥接式采集

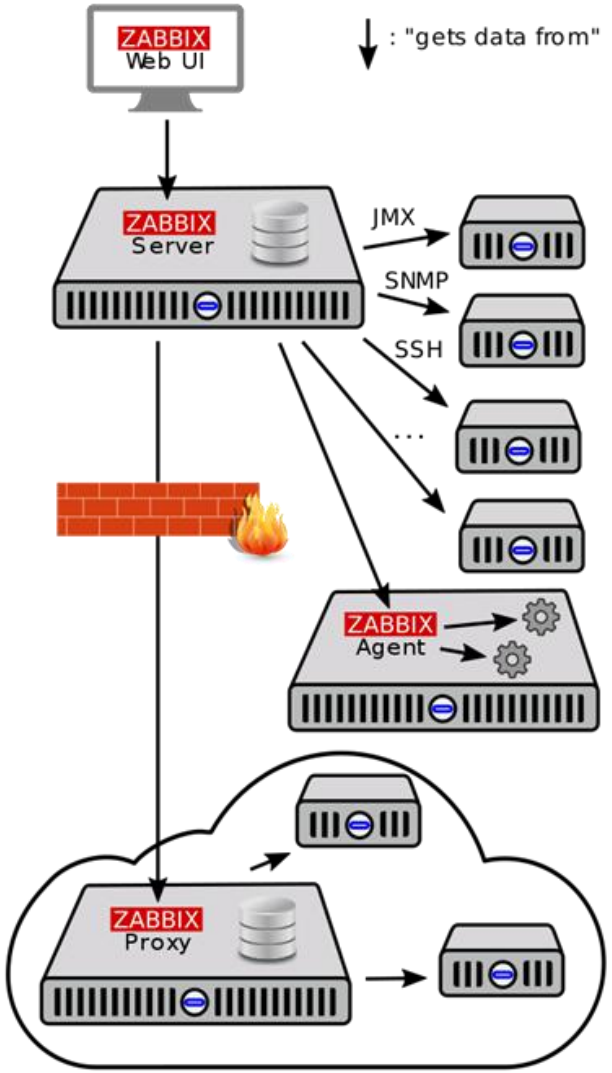
第二部分

业内解决方案

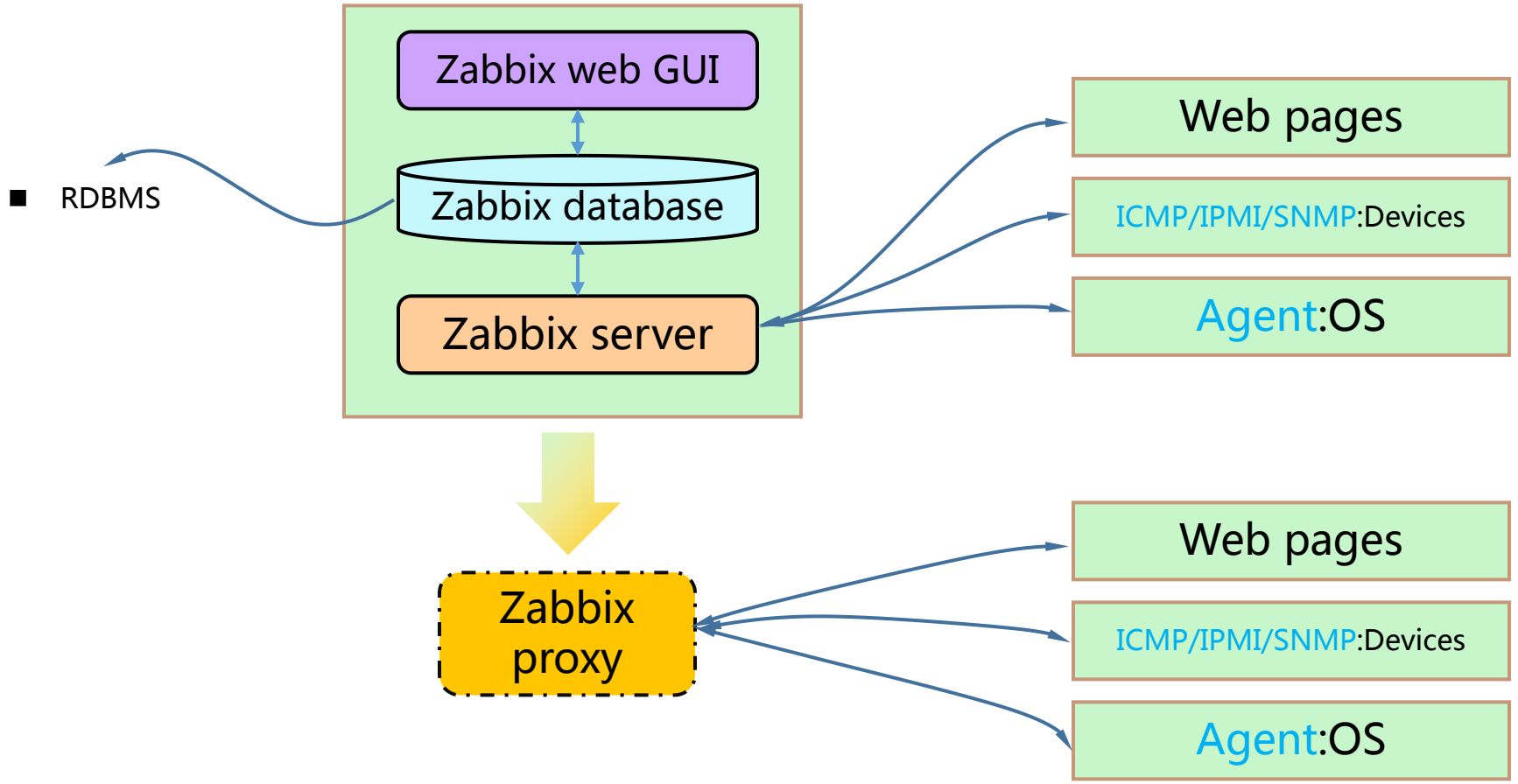
知名监控软件

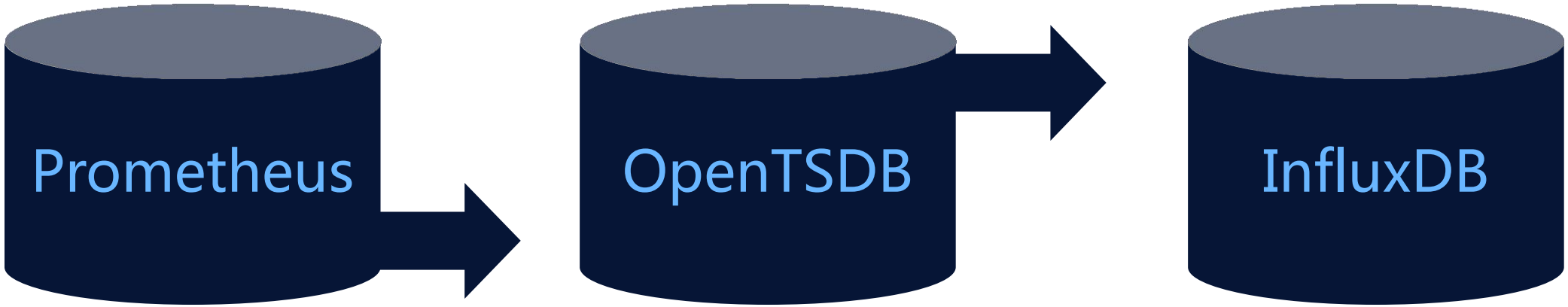

警告阈值
紧急阈值
通知升级
采集数据
保存数据
数据展示
数据分析及报警
rrd数据库
Cacti
报警工具
分析依赖关系
重点关心正常与否的状态
Nagios
（ https://www.nagios.org/ ）
Opsview
Icinga
Ntop
整合cacti和Nagios
服务发现
Zabbix
普罗米修斯
（ Prometheus ）
友盟
（ https://www.umeng.com/ ）
监控软件
监控宝
（ https://www.jiankongbao.com/ ）
云计算监控
（阿里云、腾讯云）

Zabbix物理架构图

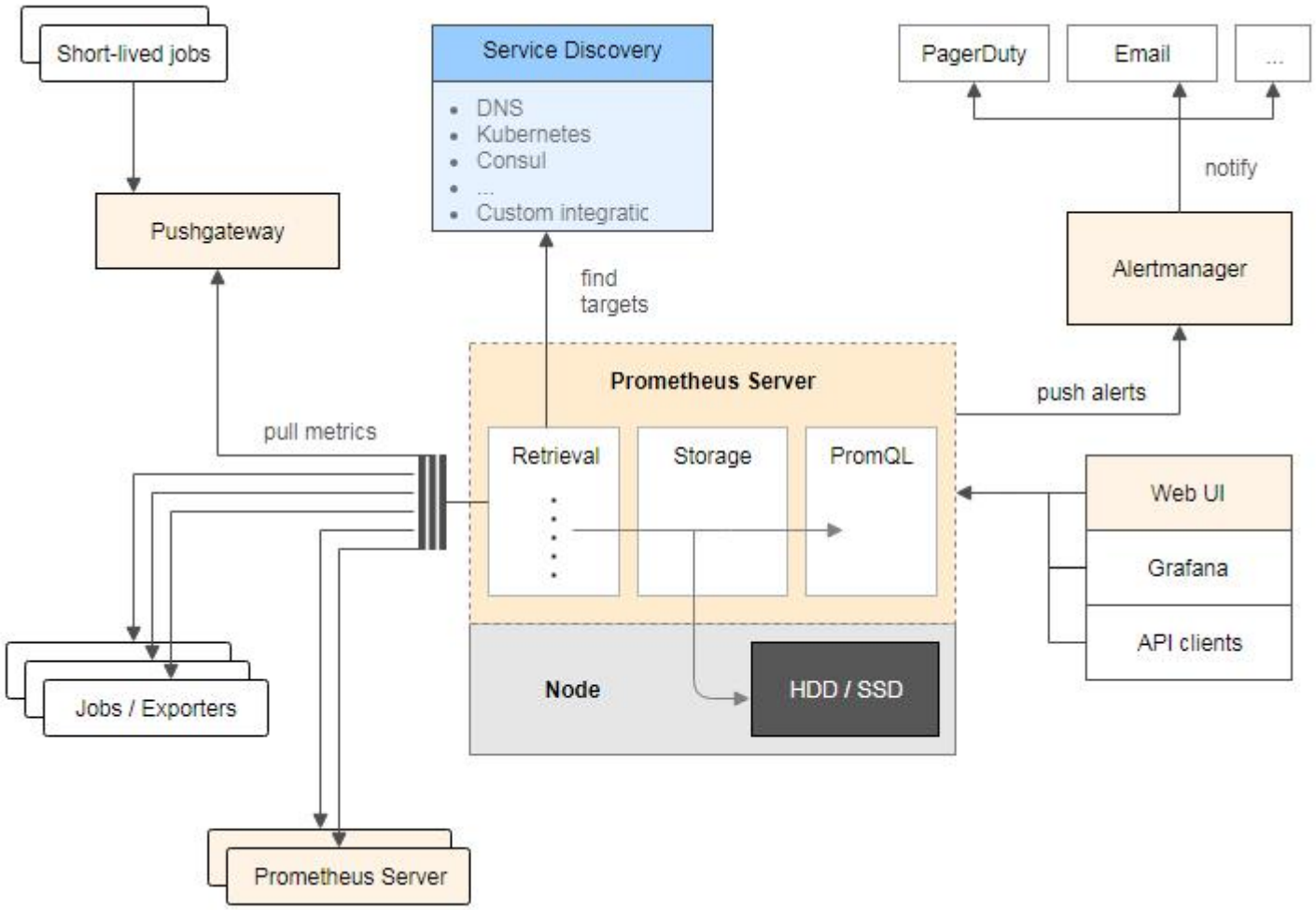


Zabbix逻辑架构图



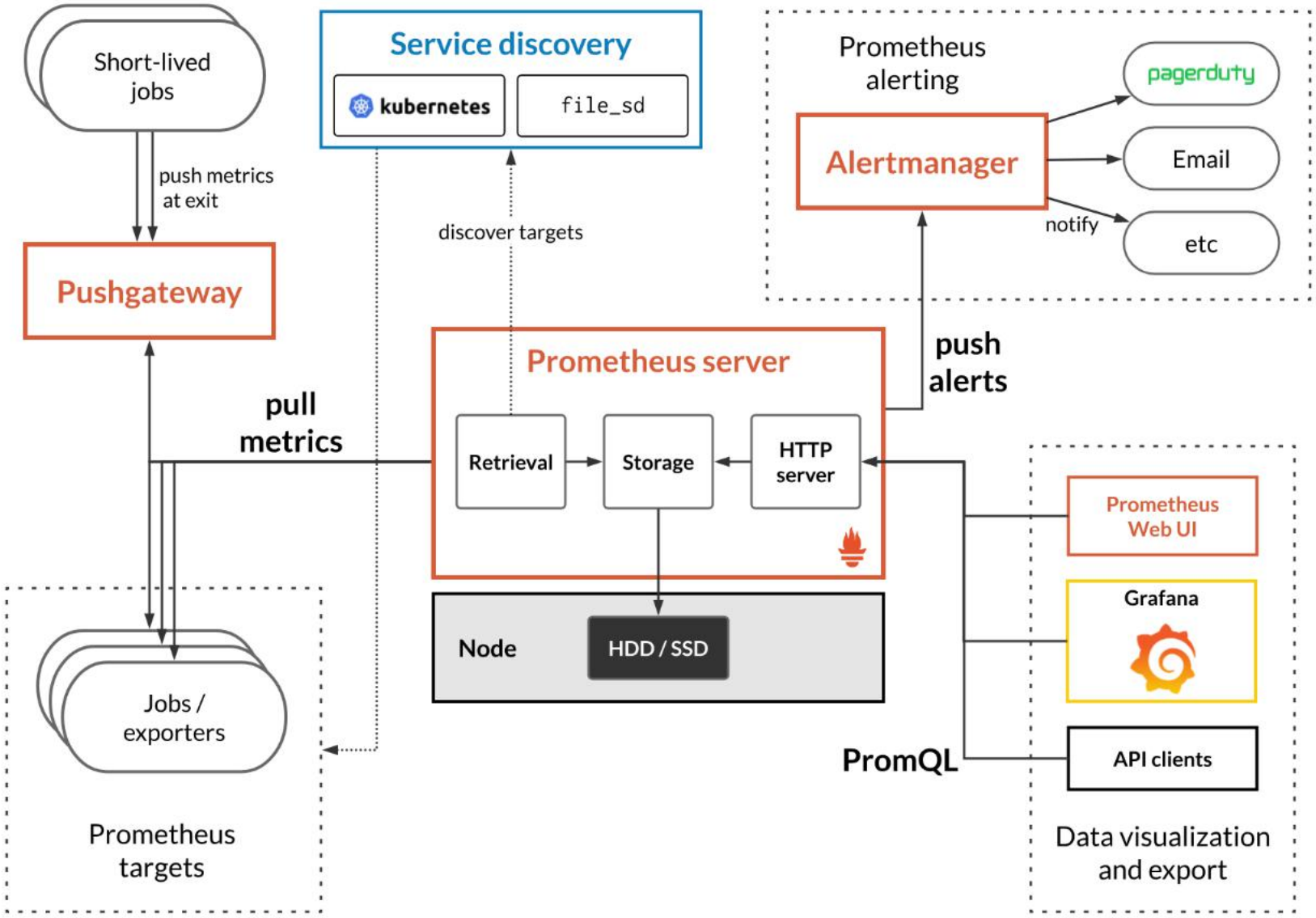

Prometheus
OpenTSDB
InfluxDB

prometheus架构图



prometheus是一个云计算基础项目，是一个系统和服务监控系统。它在给定的时间间隔内从配置的目标收集指标，计算规则表达式，显示结果，如果某些条件被观察到为真，则可以触发警报。

prometheus架构图



Prometheus简介

Prometheus可以通过在应用里进行埋点后Pull到Prometheus Server里，如果应用不支持埋点，也可以采用exporter方式进行数据采集。

对于一些定时任务模块，因为是周期性运行的，所以采用拉的方式无法获取数据，那么Prometheus也提供了一种推数据的方式，但是并不是推送到Prometheus Server中，而是中间搭建一个Pushgateway，定时任务模块将metrics信息推送到这个Pushgateway中，然后Prometheus Server再依然采用拉的方式从Pushgateway中获取数据。

需要拉取的数据既可以采用静态方式配置在Prometheus Server中，也可以采用服务发现的方式（即图的中上方Service discovery所示）

一条经验法则为，**总内存用量不应超过物理内存大小的三分之二。**

下表计算了若干典型的内存用量（假设所有节点均为 Node Exporter 节点）：

节点数目	内存留存	抓取间隔	活跃样本量	排队样本量	内存用量	物理内存
100	6h	1s	1.789G	2.237G	4.026G	6G
100	6h	5s	0.358G	0.447G	0.805G	1.5G
1000	6h	5s	3.58G	0.447G	4.027G	6G
100	24h	1s	7.156G	2.237G	9.393G	14G
100	24h	5s	1.432G	0.447G	1.879G	3G
1000	24h	5s	14.32G	0.447G	14.75G	22G

```
curl localhost:9100/metrics
```

Centos时区同步

1.设置时区
timedatectl set-timezone Asia/Shanghai

2.时间同步
crontab –e
* * * * * ntpdate –u cn.pool.ntp.org

第三部分

业内参考案例

7X24持续监控

7x24

网站可用性监控

1秒

发现故障定位问题


支持公网/内网多协议监控
支持主流网络传输协议
全面问诊网络业务健康
Ping
HTTP/HTTPS
FTP
SMTP
DNS
TCP/UDP
Traceroute

网络链路质量监控

300+

全球分布式监测节点

1分钟

持续感知链路质量

网站监控功能列表

功能	说明
仪表盘	智能筛选监控数据，实时呈现在线业务关键指标
监控任务数	可通过后台系统管理配额
历史快照	留存监控快照数据，为排障提供数据支撑
监控频率	最快可达1分钟
数据报表	实时数据统计，呈现不同维度的统计分析数据
项目对比	不同项目在同视图中进行多指标横向对比
同期对比	同一项目不同时期多指标对比
自定义告警	可灵活的设置告警阈值，制订告警规则
多用户管理	可按照业务部门或组织结构灵活管理用户
权限管理	数据及功能权限分级管控
告警处理	具有告警压缩及强大的告警能力
消息推送	可通过邮件、短信、语音、APP推送等渠道发送告警消息
URL回调	可将告警消息回调，方便客户灵活处理
监控大屏	通过大屏展示实时监控数据

全景页面性能分析

准确定位元素级性能问题

支持多维度网页故障诊断

实时发现页面错误

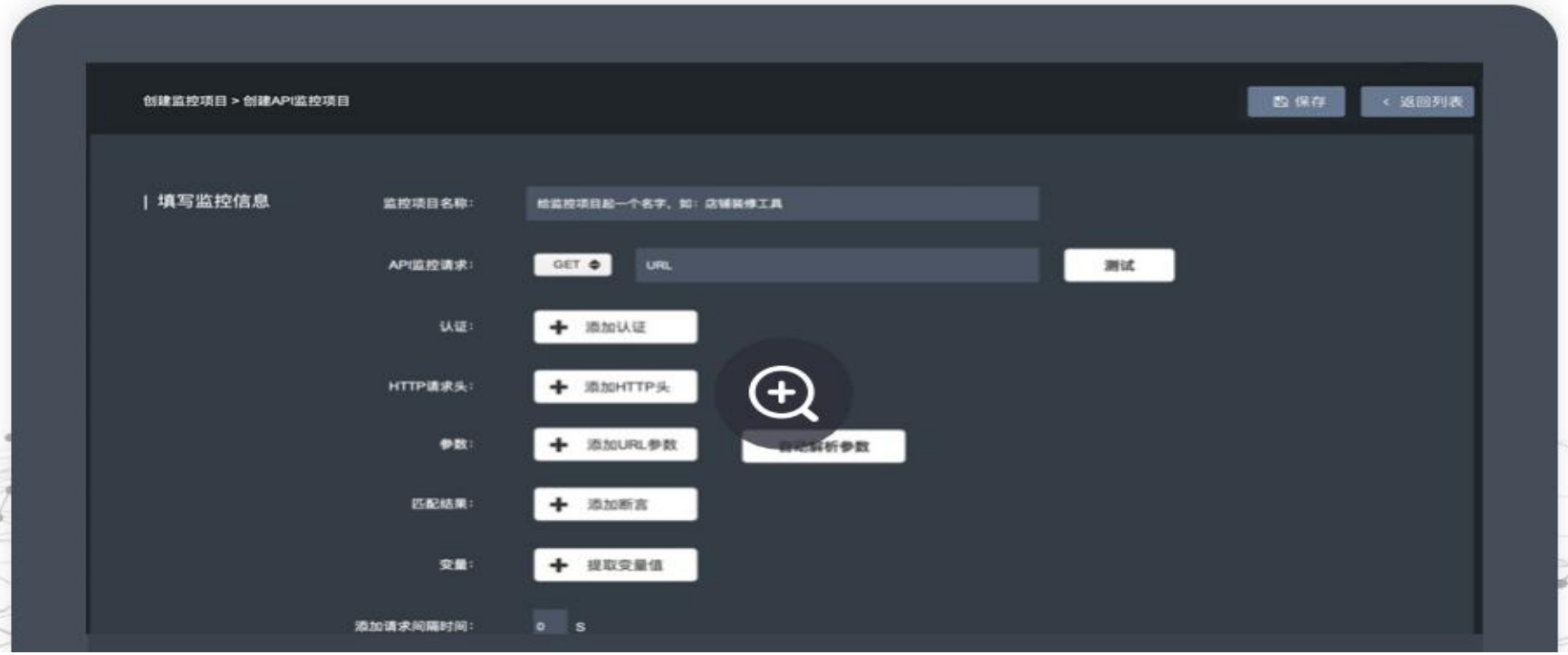
页面性能监控功能列表

功能列表	说明
仪表盘	智能筛选监控数据，实时呈现在线业务关键指标
监控任务数	可通过后台系统管理配额
元素瀑布图	留存监控快照数据，保留元素瀑布图，保留检测时的真实现场
监控频率	最快可达5分钟
元素性能评估	从多个指标及维度评估每个请求元素的性能
CDN分析及评估	评估加速效果，Cache节点响应性能、可用率、分布情况及调度策略等
数据报表	实时数据统计，呈现不同维度的统计分析数据
竞品对比	不同项目多指标在同视图或界面中横向对比
快速检测	可即时发起项目检测，方便、快捷呈现测量结果
自定义告警	可灵活设置告警阈值，制订告警规则
多用户管理	可按照业务部门或组织结构灵活管理用户
权限管理	数据及功能权限分级管控
消息推送	可通过邮件、短信等渠道发送告警消息

六种请求方式，三重性能指标

GET、POST、PUT、DELETE、
HEAD、OPTIONS

可用性、正确性、响应时间



API监控功能列表

功能	说明
全类型API监控	支持GET、POST、PUT、Delete、HEAD、OPTIONS六种方式
脚本录入	支持POSTMAN格式导入脚本，便捷创建任务
监控任务数	可通过后台系统管理配额
历史快照	留存监控快照数据，为排障提供数据支撑
监控频率	最快可达2分钟
自定义告警	可灵活的设置告警阈值，制订告警规则
多用户管理	可按照业务部门或组织结构灵活管理用户
权限管理	数据及功能权限分级管控
告警处理	具有告警压缩及强大的告警能力
消息推送	可通过邮件、短信、语音、APP推送等渠道发送告警消息
URL回调	可将告警消息回调，方便客户灵活处理

掌控全局基础设施运行状态

支持多平台环境及
主流服务器、存储、网络设备

实时采集与分析
近千项性能指标

支持多维度数据报表
与多通道智能告警