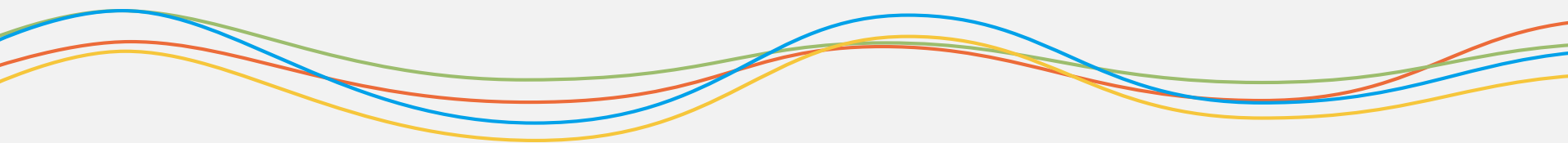


# 构建立体化的监控体系

## 58集团监控实践

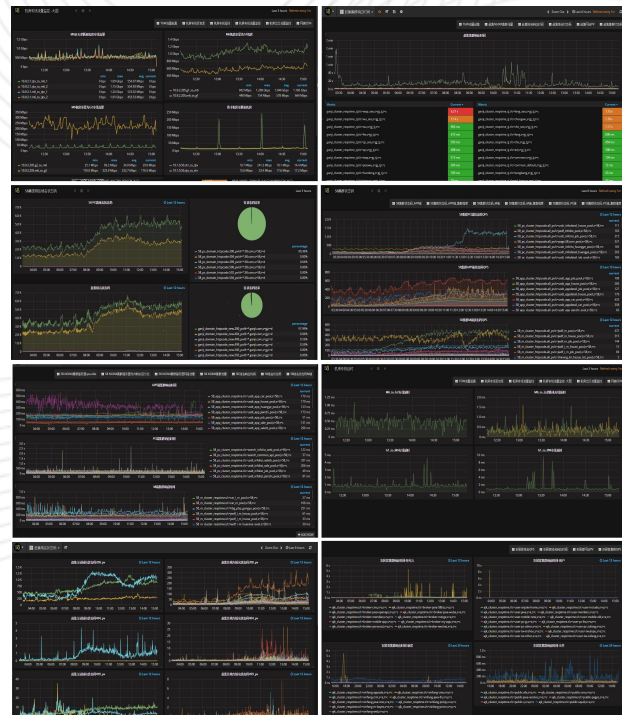
58集团-技术工程平台群-龚诚



- 龚诚
- 现任职于58集团，技术工程平台群，高级技术经理；
- 硕士毕业于哈尔滨工业大学，计算机应用专业；
- 曾任职于百度、新浪微博等公司；
- 负责运维及自动化团队的技术和管理工作；
- 在网站的稳定性建设、网站优化等方面有丰富的经验。

- 如何快速获得监控收益
- 构建立体化的监控体系
- 提升监控系统用户体验
- 智能化监控和告警信息

- 线上服务的守护神，服务稳定性的重要保障
- 运维和研发、测试人员的眼睛，快速发现和排查故障
- 将运维数据进行量化和可视化，便于对网站优化



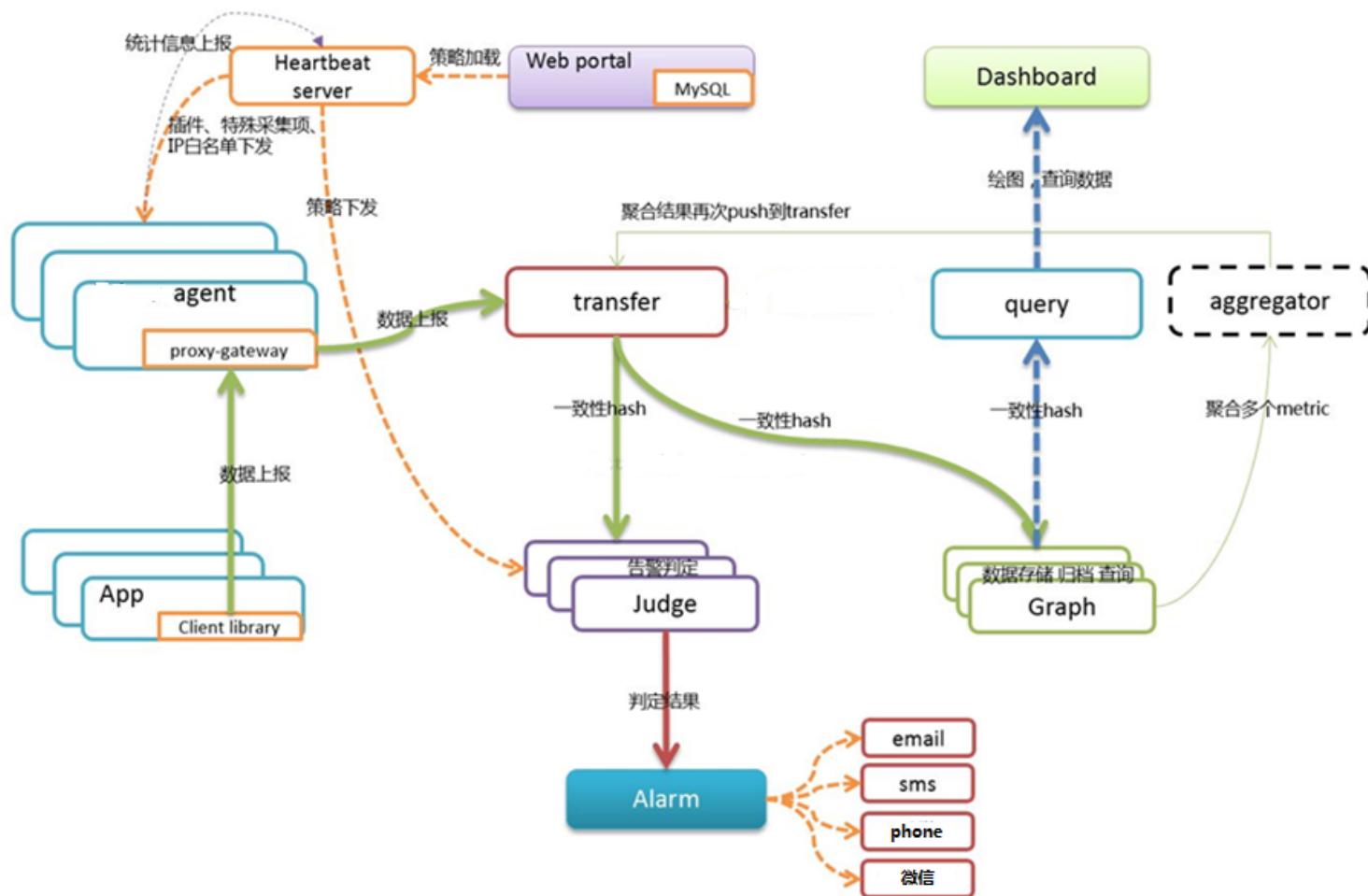
# 第一阶段

# 如何快速获得监控收益

- 监控系统数量多
- 告警数量非常多
- 监控覆盖度不够
- 监控添加很繁琐
- 应用监控难添加
- 难以辅助定位故障
- 监控运行情况未知

- 监控业务模型
  - 对集群的监控
  - 支持模板和模板的继承
  - 模板中包含多条监控策略
  - 支持告警组
- 监控系统要求
  - 高稳定性，分布式系统，有容错能力
  - 性能强大，横向可扩展，无性能瓶颈
  - 单个模块逻辑简单，方便二次开发

- 以开源监控系统为基础，进行二次开发
- 监控系统选型：open-falcon





- 监控切换到open-falcon
  - 解决部分服务器无监控问题
  - 解决告警发送数量过多问题
  - 解决异常告警的接收人问题
- 快速添加监控
  - 便于技术人员快速添加监控，提升易用性和监控添加效率
  - 一个页面添加集群名、机器列表、监控策略、告警接收人后即完成监控添加
  - 可自定义集群、模板、告警接收人
  - 对关键集群都增加了系统和应用层监控，保证了关键服务的稳定性

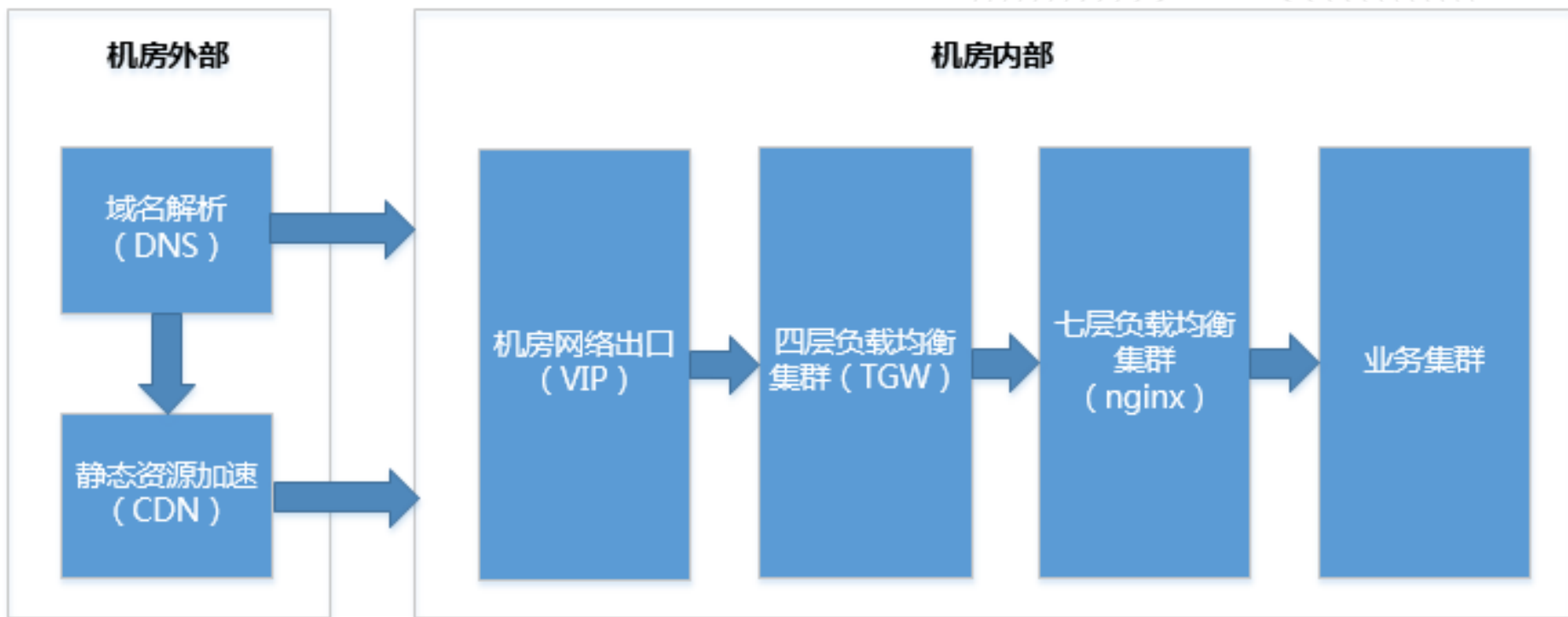
- 自动添加系统监控
  - 从CMDB同步信息，为各集群自动添加基础监控
  - 所有集群的模板继承公共的系统监控模板
  - 告警发给各集群对应的运维和研发负责人
  - 从自动部署系统同步端口号添加端口监控
  - 可自定义监控指标
- 加强功能、提升易用性
  - 监控配置：方便添加常用监控
  - 数据查看：便于查看监控数据，监控视图，监控墙
  - 告警查看：告警信息，告警历史，告警统计
  - 异常查看：当前异常，我的异常
- 监控推广
  - 帮助文档
  - 监控系统宣讲

## 第二阶段

# 构建立体化的监控体系

# 构建立体化的监控体系

- 网站总体架构图



- 网络层
  - 网络设备宕机，资源使用率，流量，服务质量，专线等
- 服务器层
  - 宕机，无法登陆，硬件故障等
- 系统层
  - 资源使用率（CPU、内存、磁盘、网络等）
- 应用层
  - 端口存活，进程存活，接口状态，服务QPS等
- 业务层
  - 订单量，成交额等业务指标

## 集群和服务器

业务层

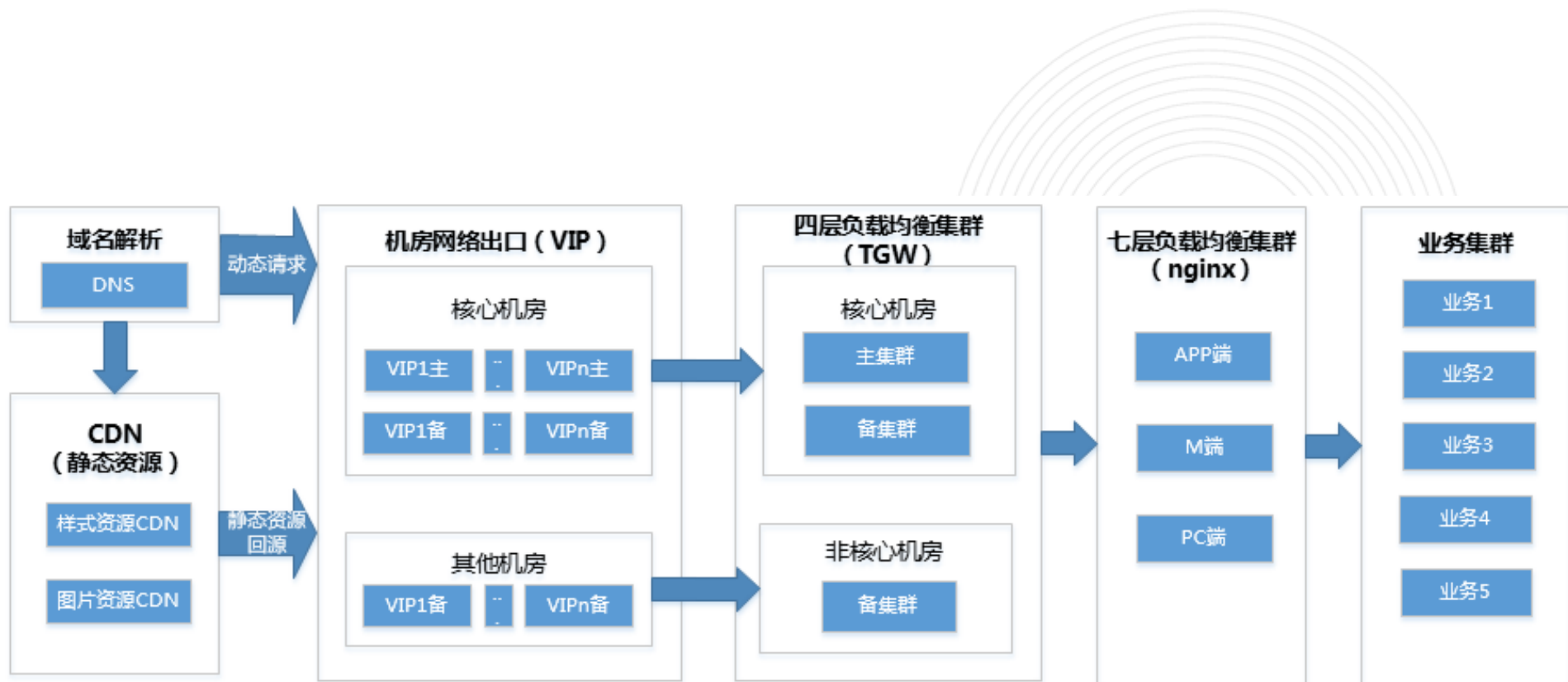
应用层

系统层

服务器层

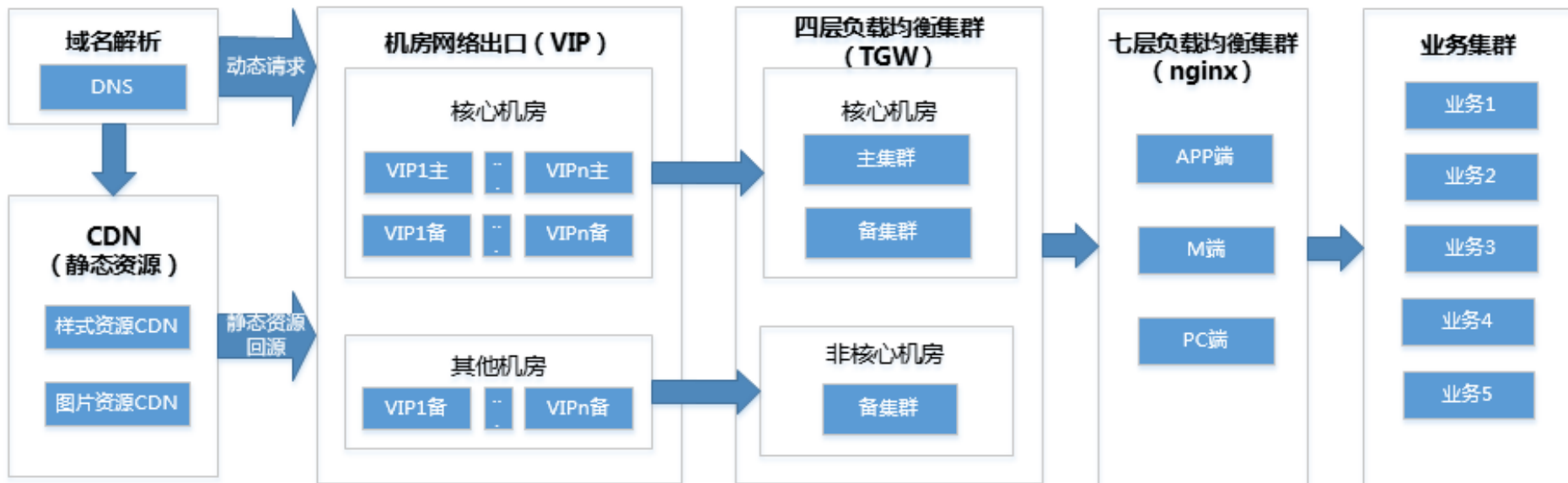
网络层

# 构建立体化的监控体系-横向



- 用户端
  - 重点页面关键指标：首屏时间，全部加载时间，可用性等
  - DNS劫持，链路劫持，页面出错，页面超时
- 机房网络出口端
  - VIP连通性监控
  - 页面监控，接口监控
- 流量接入端
  - TGW（四层网络）网络流量，是否受到攻击等
  - Nginx（七层网络）域名维度、集群维度；用户维度、集群维度
- 业务集群端
  - 单机监控（纵向：服务器层，系统层，应用层，业务层）
  - 集群监控（页面、接口监控，Nginx日志监控；可用性，响应时间）

- 监控纵向覆盖
  - 宕机监控，硬件监控，系统监控，应用监控，业务监控，网络监控
- 监控横向覆盖
  - 用户端监控、机房网络出口监控、页面和接口监控
  - 流量接入端监控、业务端监控





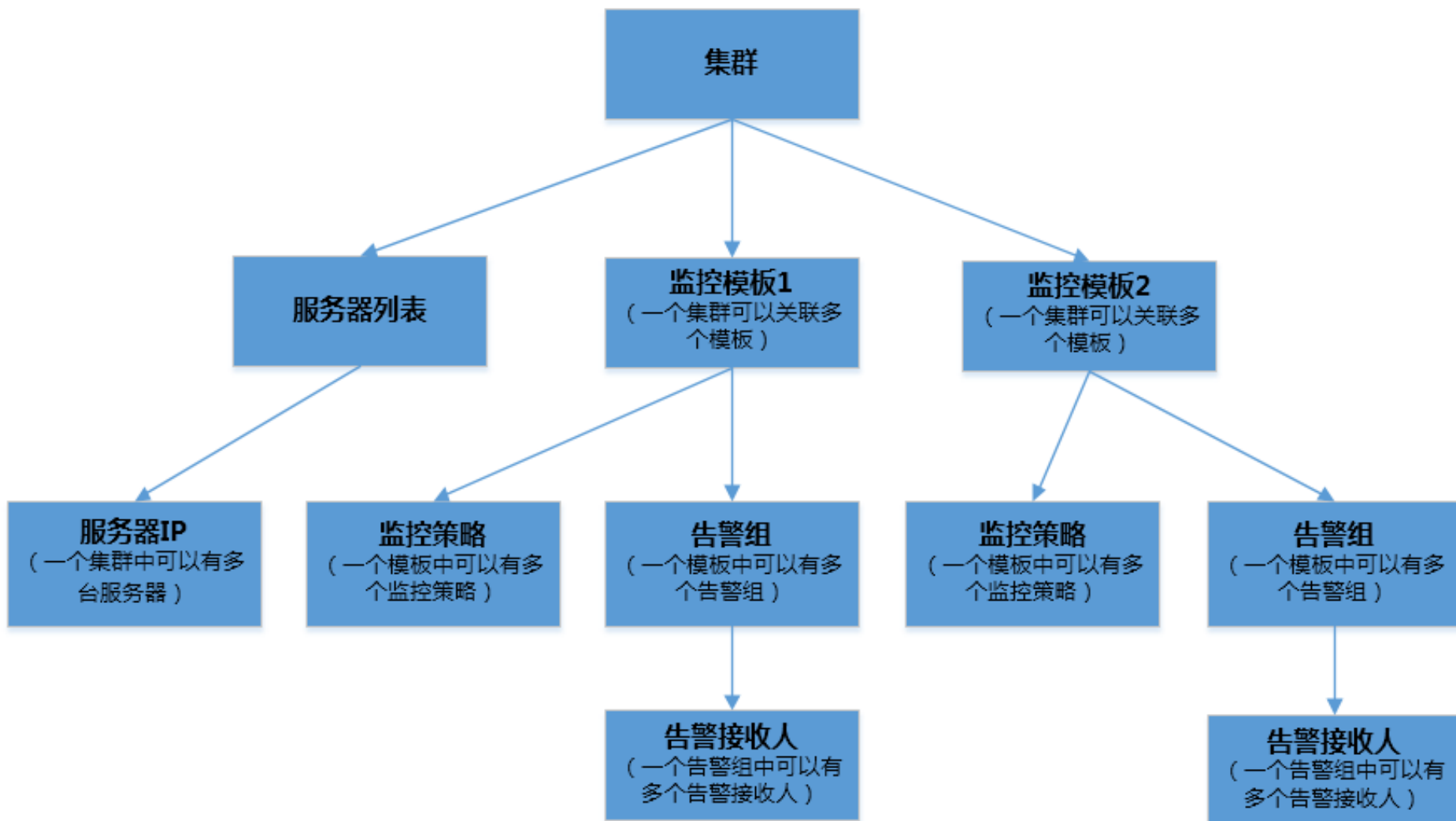
- 立体化的监控体系
  - 从横向和纵向两个维度构建起立体化监控体系
  - 提升了全局监控覆盖率
- 更强大的功能
  - 监控添加：自动添加监控，方便配置监控
  - 数据查看：查看指定指标，查看服务器负载
  - 数据视图：关键指标查看，个性化数据查看
  - 告警查看：当前异常查看，最近告警查看
- 运营质量评估
  - 业务集群端
  - 机房网络出口端
  - 用户端

# 第三阶段

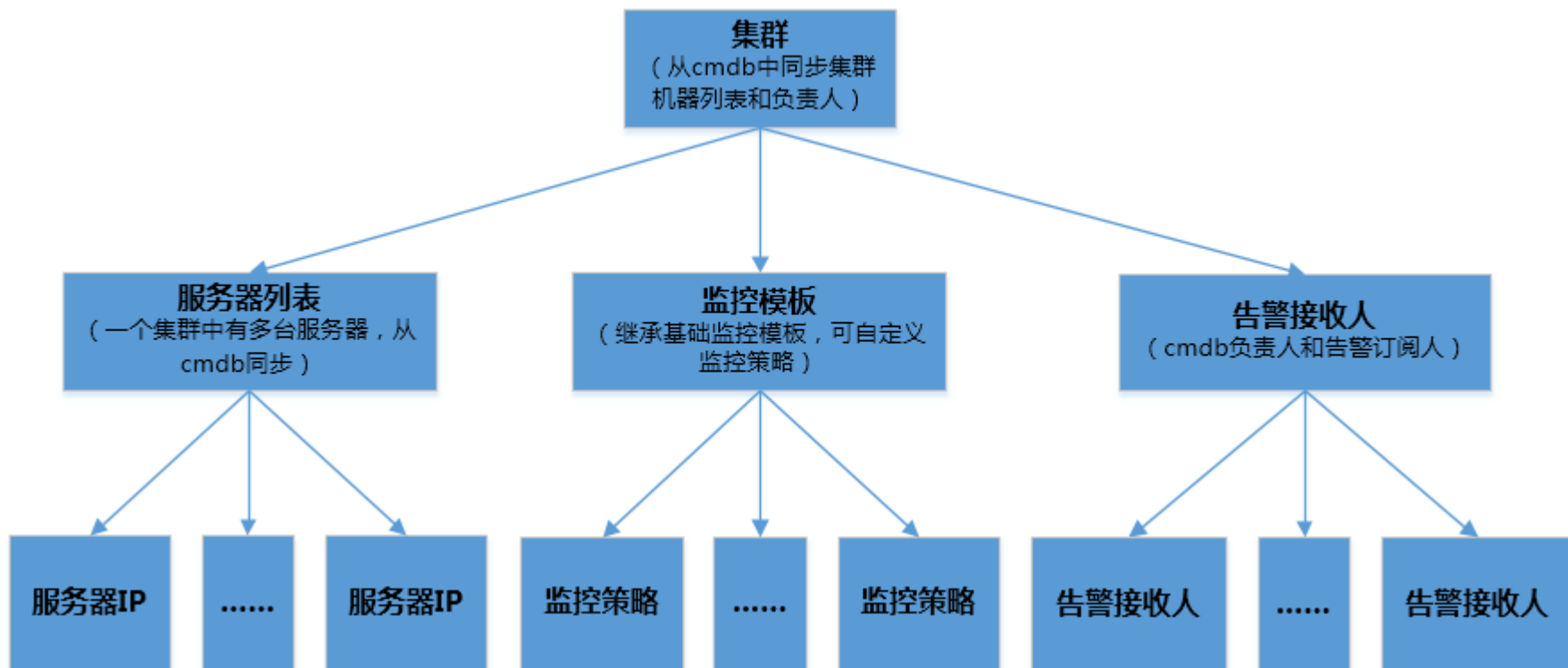
# 提升监控系统用户体验

- 完善的用户体验
  - 简化监控管理模型
    - 服务器列表、监控策略、告警接收人都关联到集群
    - 维护好上述信息即完成监控维护
  - 服务树模型
    - 所有业务与服务树节点关联
  - 统一web框架
    - 通过服务树节点选择业务范围
    - 通过菜单选择使用的功能
  - 监控相关系统整合
    - open-falcon , nginx日志监控
    - 网络监控 , 用户端监控 , IDC出口监控 , 运营质量

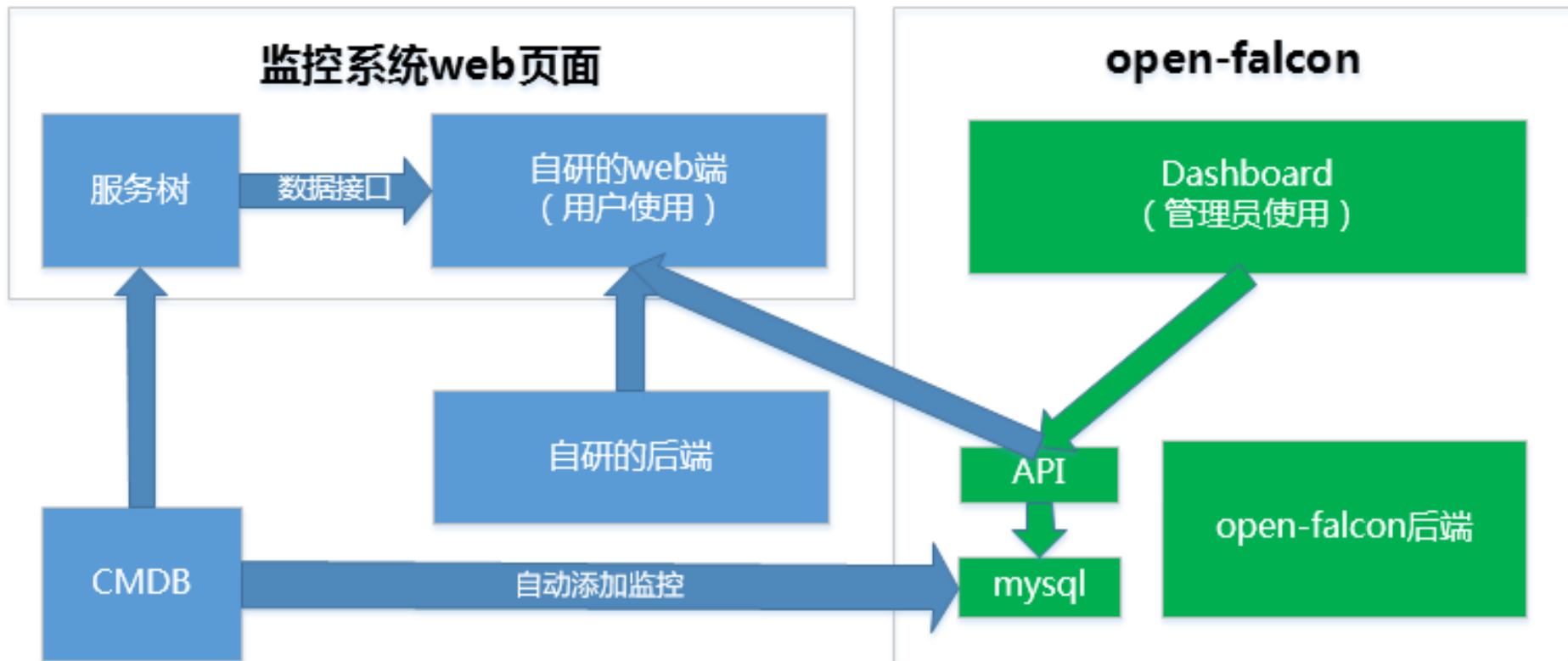
- 服务器列表和监控模板都与集群关联



- 所有监控配置项与服务树节点（集群）关联
- 监控配置项：服务器列表，监控模板，告警接收人



- 各模块逻辑关系
- 二次开发代码的可维护性



- 统一的web框架和服务树模型

58集团监控系统

我的监控 监控数据 监控配置 告警查询 容量管理 运营质量 网络出口监控 用户端监控 欢迎 gongcl

请输入节点名称/服务器IP 搜索 58集团 > 节点类型：事业群

可以输入多个关键字, 空格分割 过滤 反向过滤 标记选中部分为已解决 按时间排序 无走时刷新  我的告警

<input type="checkbox"/>	告警次数	监控指标	监控策略	告警接收人	告警时间
<input type="checkbox"/>	PROBLEM P6 [第1次/最多3次] [处理异常]	10.1...8.201/load.1min [查看数据][集群]	all(#10) 96.29 > 50 负载过高 [模版]	lig...ang	4分钟前 2017-08-07 16:49:00
<input type="checkbox"/>	PROBLEM P6 [第1次/最多3次] [处理异常]	10.1...219/load.1min [查看数据][集群]	all(#10) 88.9 > 50 负载过高 [模版]	lig...ang	5分钟前 2017-08-07 16:48:00
<input type="checkbox"/>	PROBLEM P6 [第1次/最多3次] [处理异常]	10.1...81/load.1min [查看数据][集群]	all(#10) 114.01 > 50 负载过高 [模版]	lig...ang	6分钟前 2017-08-07 16:47:00
<input type="checkbox"/>	PROBLEM P6 [第1次/最多3次] [处理异常]	10.1...4.68/load.1min [查看数据][集群]	all(#10) 90.67 > 50 负载过高 [模版]	lig...ang	6分钟前 2017-08-07 16:47:00
<input type="checkbox"/>	PROBLEM P6 [第1次/最多3次] [处理异常]	10.1...199/load.1min [查看数据][集群]	all(#10) 133.97 > 50 负载过高 [模版]	lig...ang	6分钟前 2017-08-07 16:47:00

# 一、监控配置

- 服务器列表

[58集团](#) > [某某公司](#) > [某某部](#) > [某某n\\_scf\\_zzesextra](#)

节点类型：集群

 已设置维护

服务器IP	维护起始时间	维护截止时间	关联操作
10.1.1.155			所属集群
10.1.1.156			所属集群
10.1.1.157			所属集群
10.1.1.158			所属集群
10.1.1.159			所属集群
10.1.1.176			所属集群
10.1.1.177			所属集群
10.1.1.178			所属集群
10.1.1.179			所属集群

共计：9，每页：



# 一、监控配置

- 监控的策略

58集团监控系统

我的监控 监控数据 监控配置 告警查询 容量管理 运营质量 用户端监控 欢迎 gongcheng !

请输入节点名称/服务器IP 搜索

58集团 > 转... > ... > ... web 节点类型：集群

模板基本信息

模板名：...\_web | 父模板：...\_cluster.base

该模板中的策略列表

告警级别：(0:语音,短信,邮件告警; 1,2:短信,邮件告警; 3,4,5,6: 邮件告警)

告警升级：常规状态下未处理的告警信息会自动提升告警级别, 升级后的告警会一天发一次。升级后的告警级别和人员可以自定义。

监控项/标签 [注释]	告警条件	最大告警次数	告警级别	升级告警级别	生效时间
net.port.listen/port=9033 [端口不通]	all(#3)==0	3	2	0	

模板告警配置, 对模板中的所有策略生效

告警接收组: ...\_zappapi\_web  
升级告警组: ...\_zappapi\_web

← 返回

# 一、监控配置



## 告警接收人

58集团监控系统

我的监控 监控数据 监控配置 告警查询 容量管理 运营质量 客户端监控 欢迎 gongcheng !

请输入节点名称/服务器IP 搜索

58集团 > 房产 > 房产 > app > dict

节点类型: 集群

搜索组员 订阅告警

告警组: cmdb\_组\_...\_scf\_dict

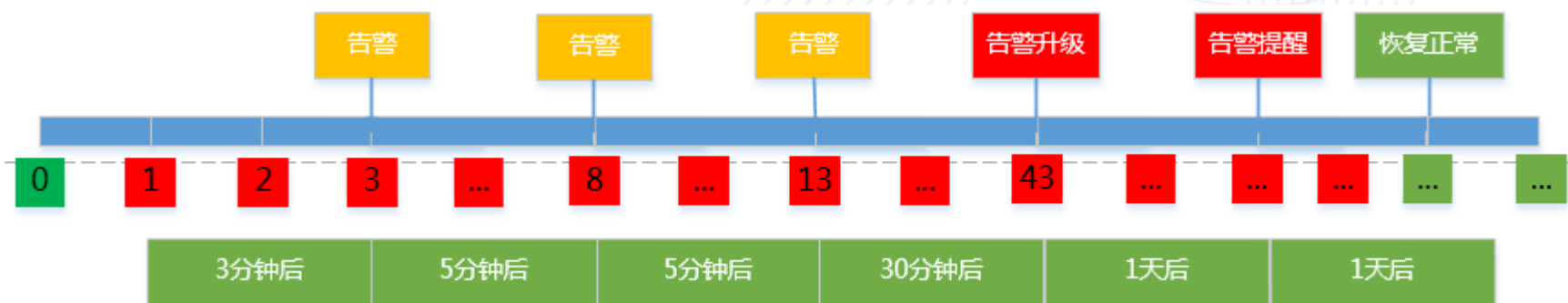
组员	手机	邮箱	来源
mazh...	136...	mazh...@...ji.com	cmdb
shen...	185...	shen...@...ji.com	cmdb
zhou...	18...	zhou...@...ji.com	cmdb
wang...	137...	wang...@...ji.com	监控系统
zhang...	15...	zhang...@...ji.com	监控系统

共计: 5, 每页: 10

返回

## 二、告警查看

- 多种告警方式
  - 告警级别：微信、邮件->短信->语音
- 告警升级，告警提醒
  - 连续3次异常则告警，告警间隔5分钟，最多告警3次
  - 30分钟后未处理则升级，1天后未处理则提醒，每天提醒1次
  - 使用升级后的告警级别，使用升级后的告警接收人



## 二、告警查看

- 当前的异常，告警查询

58集团监控系统

我的监控 监控数据 监控配置 告警查询 容量管理 运营质量 网络出口监控 用户端监控 欢迎 gongcl

请输入节点名称/服务器IP 搜索 58集团 > 节点类型：事业群

可以输入多个关键字, 空格分割 过滤 反向过滤 标记选中部分为已解决 按时间排序 无走时刷新  我的告警

<input type="checkbox"/>	告警次数	监控指标	监控策略	告警接收人	告警时间
<input type="checkbox"/>	PROBLEM P6 [第1次/最多3次] [处理异常]	10.1.1.201/load.1min [查看数据][集群]	all(#10) 96.29 > 50 负载过高 [模版]	liguang	4分钟前 2017-08-07 16:49:00
<input type="checkbox"/>	PROBLEM P6 [第1次/最多3次] [处理异常]	10.1.1.219/load.1min [查看数据][集群]	all(#10) 88.9 > 50 负载过高 [模版]	liguang	5分钟前 2017-08-07 16:48:00
<input type="checkbox"/>	PROBLEM P6 [第1次/最多3次] [处理异常]	10.1.1.81/load.1min [查看数据][集群]	all(#10) 114.01 > 50 负载过高 [模版]	liguang	6分钟前 2017-08-07 16:47:00
<input type="checkbox"/>	PROBLEM P6 [第1次/最多3次] [处理异常]	10.1.1.68/load.1min [查看数据][集群]	all(#10) 90.67 > 50 负载过高 [模版]	liguang	6分钟前 2017-08-07 16:47:00
<input type="checkbox"/>	PROBLEM P6 [第1次/最多3次] [处理异常]	10.1.1.199/load.1min [查看数据][集群]	all(#10) 133.97 > 50 负载过高 [模版]	liguang	6分钟前 2017-08-07 16:47:00

## 二、告警查看

- 最近的告警

58集团监控系统

我的监控

监控数据

监控配置

告警查询

容量管理

运营质量

用户端监控

欢迎 gongcheng !

请输入节点名称/服务

搜索

58集团

节点类型：58集团

服务器IP: 10.1.1.10

异常类型: 宕机/端口不通

用户名: OA用户名

日期: 2017-07-11

开始时间: 16:00:00

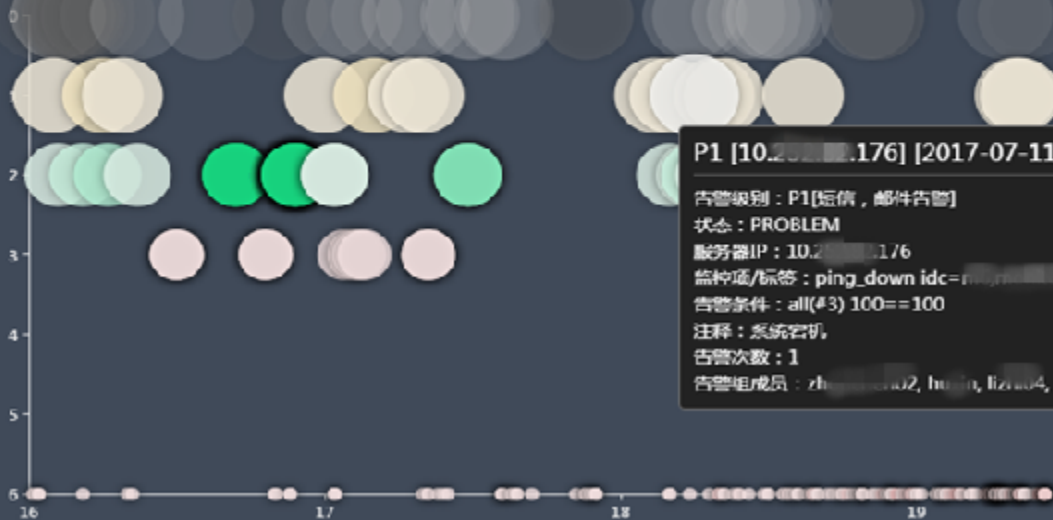
结束时间: 19:27:27

告警

P0 P1 P2 P3 P4 P5 P6

告警级别

圆形大小：告警级别



# 三、监控数据

- 查看指定指标数据：常用/高级

58集团监控系统

我的监控 | **监控数据** | 监控配置 | 告警查询 | 容量管理 | 运营质量 | 用户端监控

欢迎 gongcheng !

节点类型：集群

请输入节点名称/服务器IP 搜索

58集团 > > > jv...se

服务器IP

10.4...

空格分割多个关键字

搜索 显示50条

全选(支持shift范围选择)

<input checked="" type="checkbox"/>	10.4...95
<input checked="" type="checkbox"/>	10.4...161
<input checked="" type="checkbox"/>	10.4...167
<input checked="" type="checkbox"/>	10.4...35
<input checked="" type="checkbox"/>	10.4...38
<input checked="" type="checkbox"/>	10.4...8.39
<input checked="" type="checkbox"/>	10.4...8.42
<input checked="" type="checkbox"/>	10.4...8.43
<input checked="" type="checkbox"/>	10.4...8.46

常用  高级

概况  CPU  磁盘  磁盘IO  网络  JVM

快速过滤 看图

<input checked="" type="checkbox"/> 监控指标 (监控项+标签)	类型	频率
<input checked="" type="checkbox"/> cpu.idle	原始值	60s
<input checked="" type="checkbox"/> mem.memfree.percent	原始值	60s
<input checked="" type="checkbox"/> df.statistics.used.percent	原始值	60s

# 三、监控数据

- 生成个性化监控视图

请输入节点名称/服务器IP

搜索

58集团 > 监控数据 > 告警查询 > 告警查询

节点类型：集群

开始

结束

采样方法 AVERAGE

视角

Endpoint视角

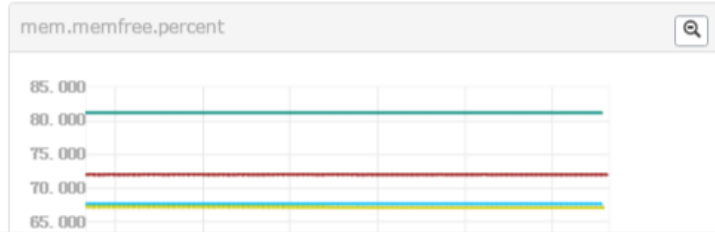
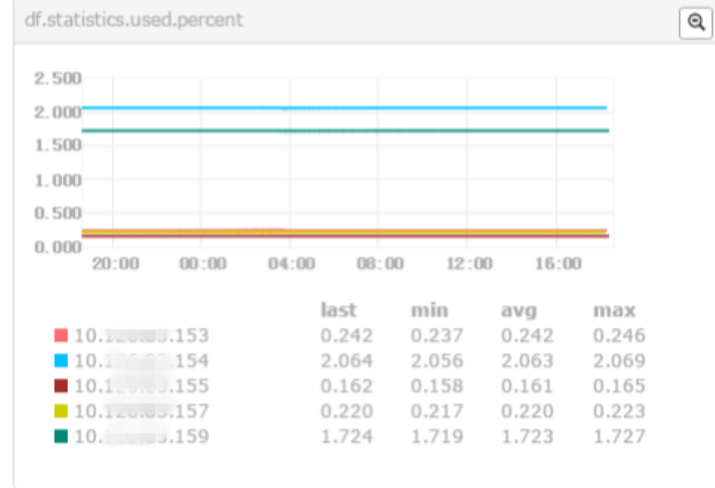
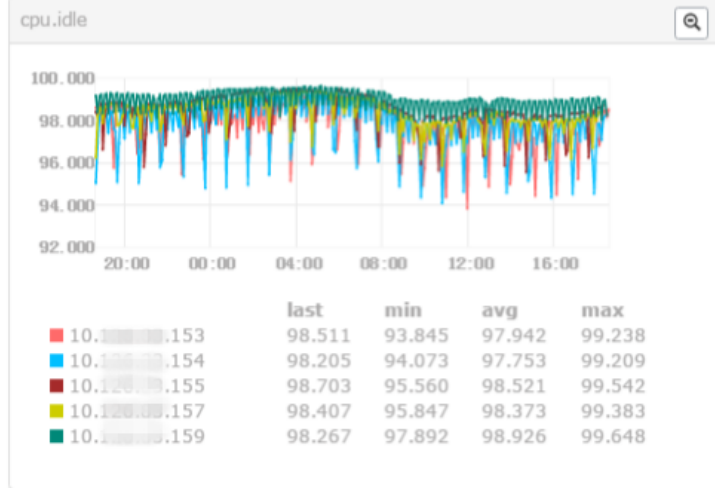
求和  快速看图

最近1天

看图

重置

生成视图



# 三、监控数据

- 收藏个性化监控视图；在“我的监控”中，点击查看我收藏的监控视图

请输入节点名称/服务器IP 搜索 58集团 > 监控数据 > 告警查询 > 容量管理 > 运营质量 > 网络出口监控 > 用户端监控 > 旧监控系统 节点类型：集群

58集团 / g... / 编辑 / 批量编辑 / 删除 / 克隆 / +graph / 隐藏legend / 布局 / 时间段 / 取消收藏

### 58monitor

cpu.idle

	last	min	avg	max
10.1...153	98.511	93.845	97.938	99.238
10.1...154	98.205	94.073	97.765	99.209
10.1...155	98.703	95.560	98.523	99.542
10.1...157	98.407	95.847	98.381	99.383
10.1...159	98.267	97.892	98.927	99.648

### 58monitor

df.statistics.used.percent

	last	min	avg	max
10.1...153	0.242	0.237	0.242	0.246
10.1...154	2.064	2.056	2.063	2.069
10.1...155	0.162	0.158	0.161	0.165
10.1...157	0.221	0.217	0.220	0.223
10.1...159	1.724	1.719	1.723	1.727

### 58monitor

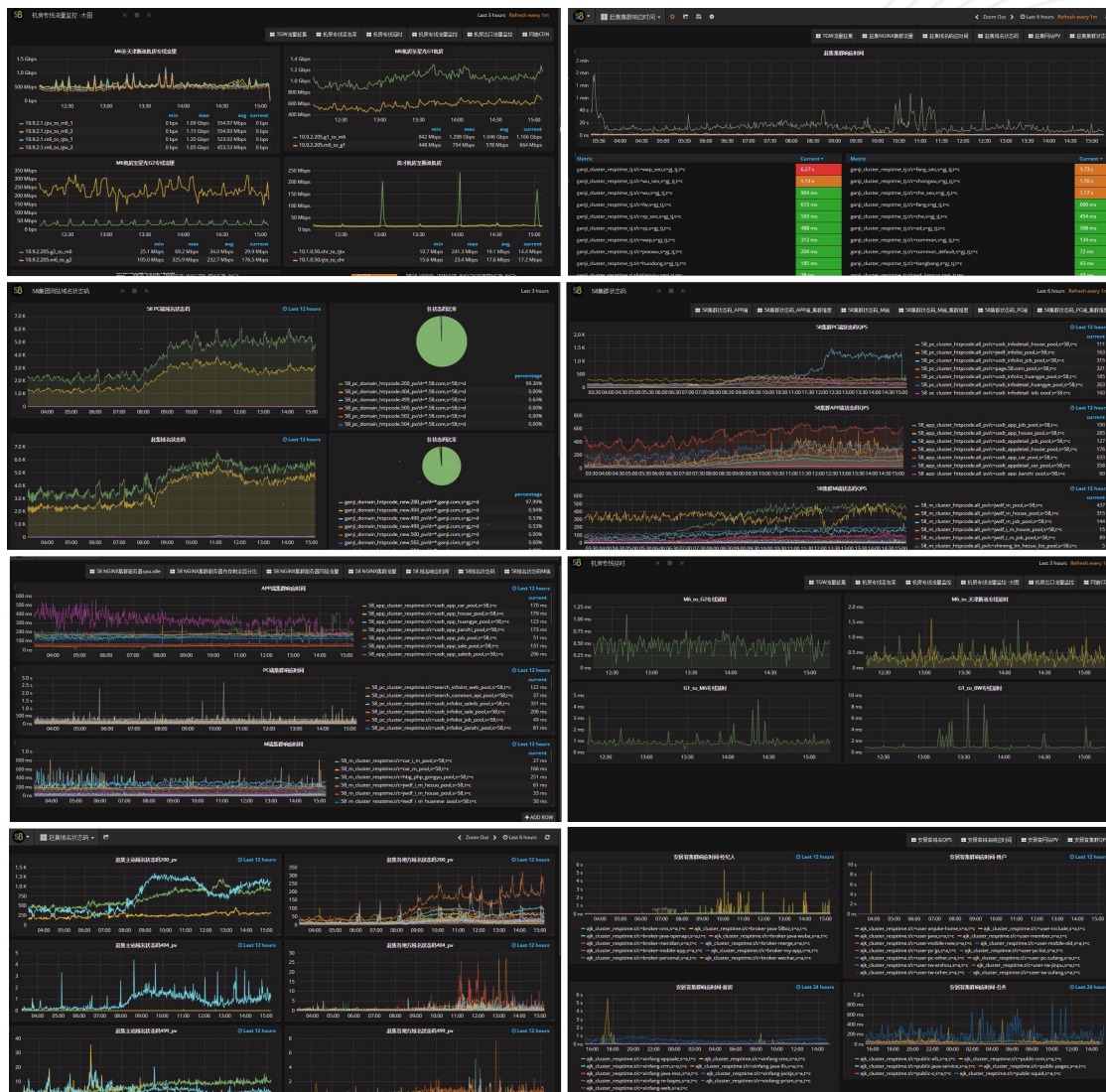
mem.memfree.percent



# 三、监控数据

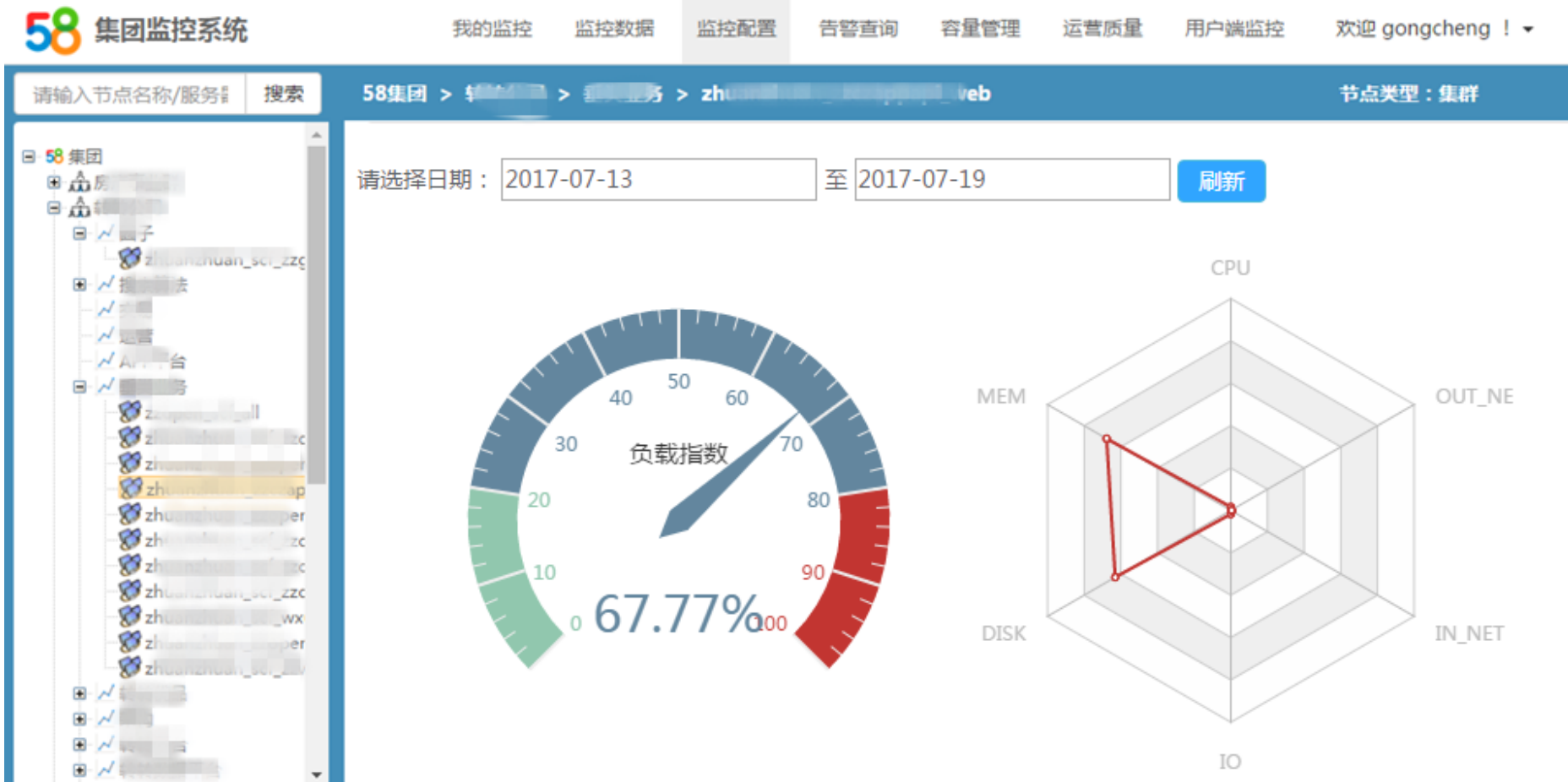


## 核心数据在监控墙中展示



# 三、监控数据

- 容量管理：服务器负载、业务负载



# 三、监控数据

- 运营质量：业务集群，机房网络出口，用户端

58集团监控系统

我的监控

监控数据

监控配置

告警查询

容量管理

运营质量

用户端监控

欢迎 gongcheng !

请输入节点名称/服务器

搜索

58集团 >

节点类型：事业群

## 集群关键指标

集群 已选15个共15个

指标

响应时间

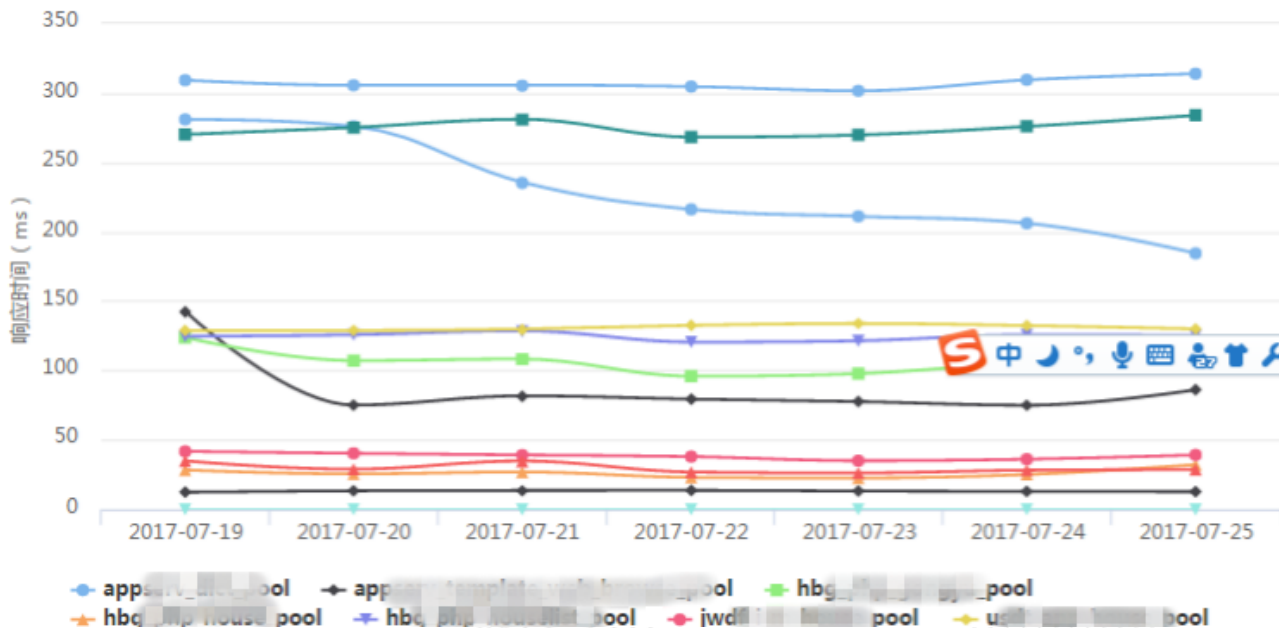
日期 2017-07-19

至

2017-07-25

查询

响应时间曲线



## 四、我的监控

- 我负责的异常，我接收的告警，我订阅的告警
- 我收藏的视图，我的集群，我的模板

58 集团监控系统

我的监控 监控数据 监控配置 告警查询 容量管理 运营质量 客户端监控 欢迎 gongcheng !

请输入节点名称/服务器IP 搜索 58集团 节点类型：58集团

搜索集群名    我的集群

路径	集群名	业务负责人
58集团. [redacted] _monitor	comp-[redacted]_src_cmdb_cluster_[redacted]_monitor	gongcheng
58集团.高 [redacted] _advance	comp-[redacted]_src_cmdb_cluster_[redacted]_advance	lisheng01
58集团. [redacted] _monitor	comp-[redacted]_src_cmdb_cluster_[redacted]_monitor	ch...
58集团. [redacted] _jankong	comp-[redacted]_src_cmdb_cluster_[redacted]_jankong	gongcheng

共计：4，每页：10

# 第四阶段

# 智能化的监控和告警信息

- 告警信息合并
  - 同机器的告警合并：宕机时会有端口、进程、接口监控告警
  - 同集群的告警合并：服务器负载高，或因接口、存储问题导致
  - 同网段的宕机告警合并：网络设备有问题导致
  - 同根因的告警合并：同一异常导致流量告警和页面、接口监控告警
- 告警信息优化
  - 微信告警：与邮件的告警级别一致
  - 告警信息的丰富化：文字（告警详情），图片（异常数据变化趋势），链接（修改监控模板，备注处理过程，相关监控数据视图）
  - 异常根源原因分析：根据运维知识库，推断异常根源原因

- 新的监控策略
  - 数据的同比环比监控：告警，数据展示
  - 数据的异常变化率监控：连续一段时间内数据突增，突降
  - 集群中异常机器比例监控：集群中超过一定比例的机器有问题
  - 组合条件的告警：多个监控指标都满足条件则告警
  - 容量监控：预测即将达到容量水位则告警
- 故障自愈
  - 服务器宕机自动处理：自动恢复，自动分配备机
  - 磁盘空间不足自动处理：删除预定义目录的文件
  - 负载升高自动扩容：调用部署系统和云平台
  - 流量自动调度：操作TGW和Nginx进行流量切换

**THANK YOU**

