

大规模集群之告警系统实践

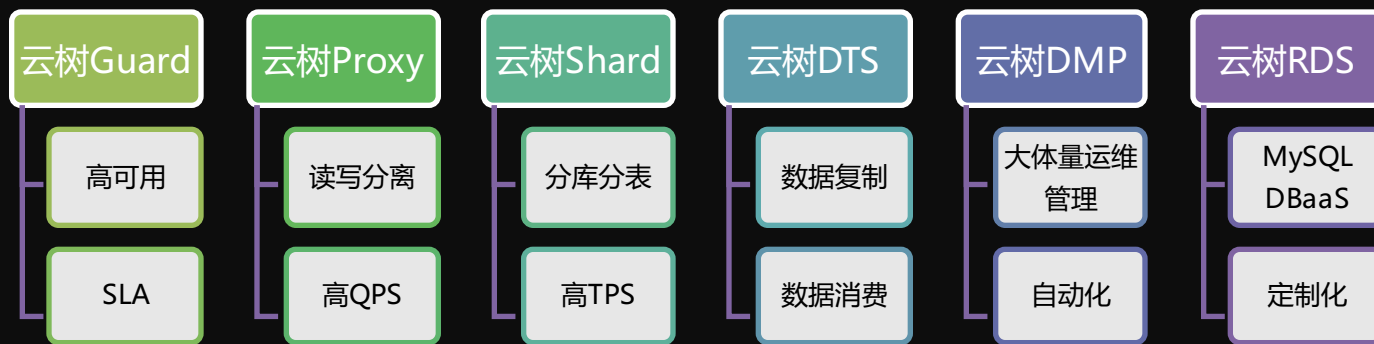
— Alertmanager

上海爱可生信息技术股份有限公司

个人介绍



我们干了啥



www.actionsky.com

目录

CONTENTS

一. 告警的选型

二. Alertmanager的实现

三. Alertmanager的实践

| 告警的选型

- 告警需求
- 方案选型

| 告警需求

- 告警的**对接**
- 告警的**收敛**
- 告警的**可用性**

| 告警需求-告警的对接

- 多样的告警源
- 多样的告警目标

| 告警需求-告警的收敛

- 告警短信多
- 关联告警多
- 运维期间不希望收到告警

| 告警需求-告警的可用性

- 告警系统的高可用
- 隔离的故障域

| 告警的选型

- 告警需求
- 方案选型

| 方案选型-备选方案

Prometheus



Zabbix

ZABBIX

Open-falcon



| 方案选型-方案对比

告警的对接

	告警源	告警目标
Zabbix	多通道	多通道
Open-falcon	多通道	多通道
Prometheus	多通道	多通道

| 方案选型-方案对比

告警的收敛

	收敛	通知次数
Zabbix	无	支持
Open-falcon	简单收敛	支持
Prometheus	灵活规则	不支持

| 方案选型-方案对比

告警的可用性

	故障域	HA
Zabbix	大	单点
Open-falcon	小	单点
Prometheus	小	HA

| 方案选型-方案对比

其他

	配置	语言
Zabbix	基于模版	C++
Open-falcon	基于模版	Go/Python
Prometheus	树形结构	Go

告警选型的背景-方案选型

	zabbix	open-falcon	prometheus
监控对象	主要监控集群	主要监控集群	主要监控集群
可扩展性	分层设计，可扩展	分层设计，可扩展	分层设计，可扩展
告警	支持告警	支持告警	支持（监控告警项目分离）
监控数据存储	MySQL / PG	MySQL + Redis + Opentsdb	Opentsdb
监控节点规模	1000+	1000+	1000+
编程语言	C++	Go + Python	Go
优点	1.成熟稳定，应用广泛 2.部署简单，运维方便 3.图形化配置	1.架构无单点 2.微服务设计思路 3.时序存储 4.支持grafana等多种展示方式	1.客户端丰富 2.google系，社区热度大 3.容器监控方案 4.支持grafana等多种展示方式
缺点	1.关系型存储，集群大容易卡慢 2.没有告警收敛	1.项目时间短，社区稳定性考验 2.架构复杂，运维成本大	1.文档相对缺位 2.监控数据保留时间短
场景	中型规模，私有云	中大型规模，私有云	中大型规模，私有云、容器

目录

CONTENTS

一.告警的选型

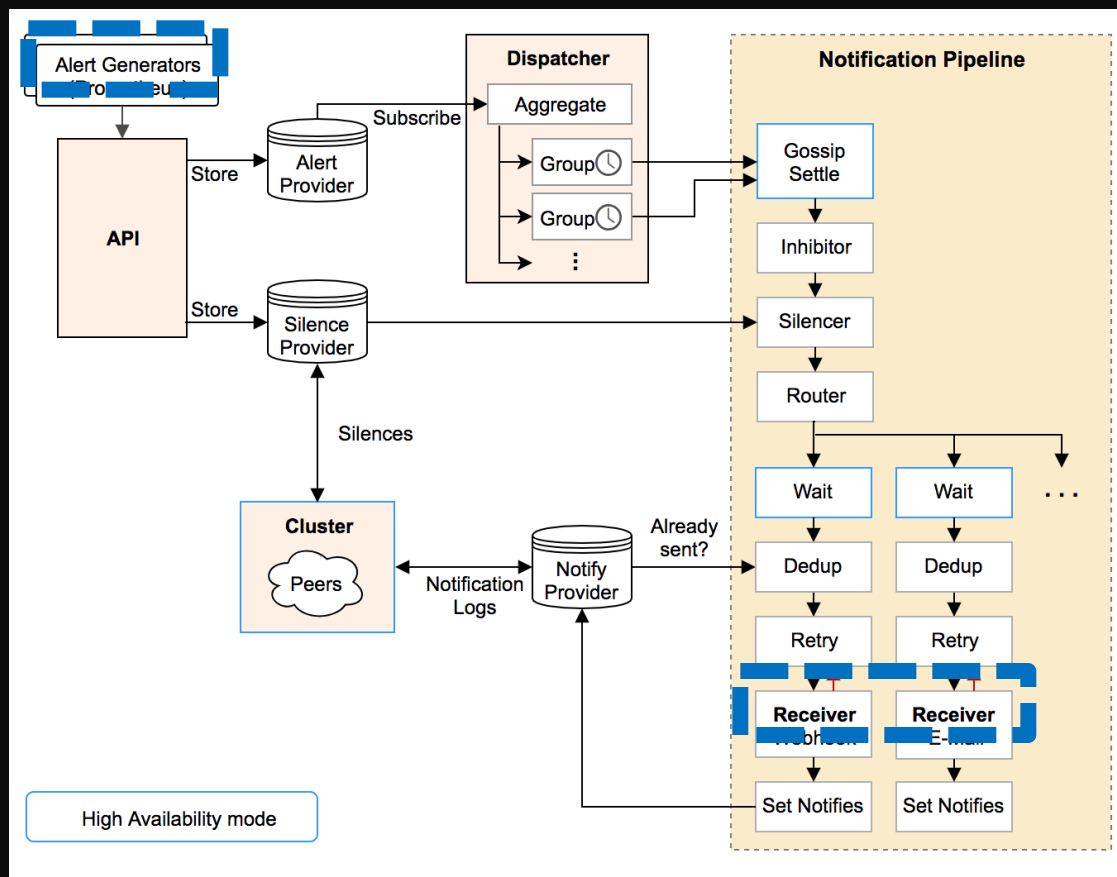
二.Alertmanager的实现

三.Alertmanager的实践

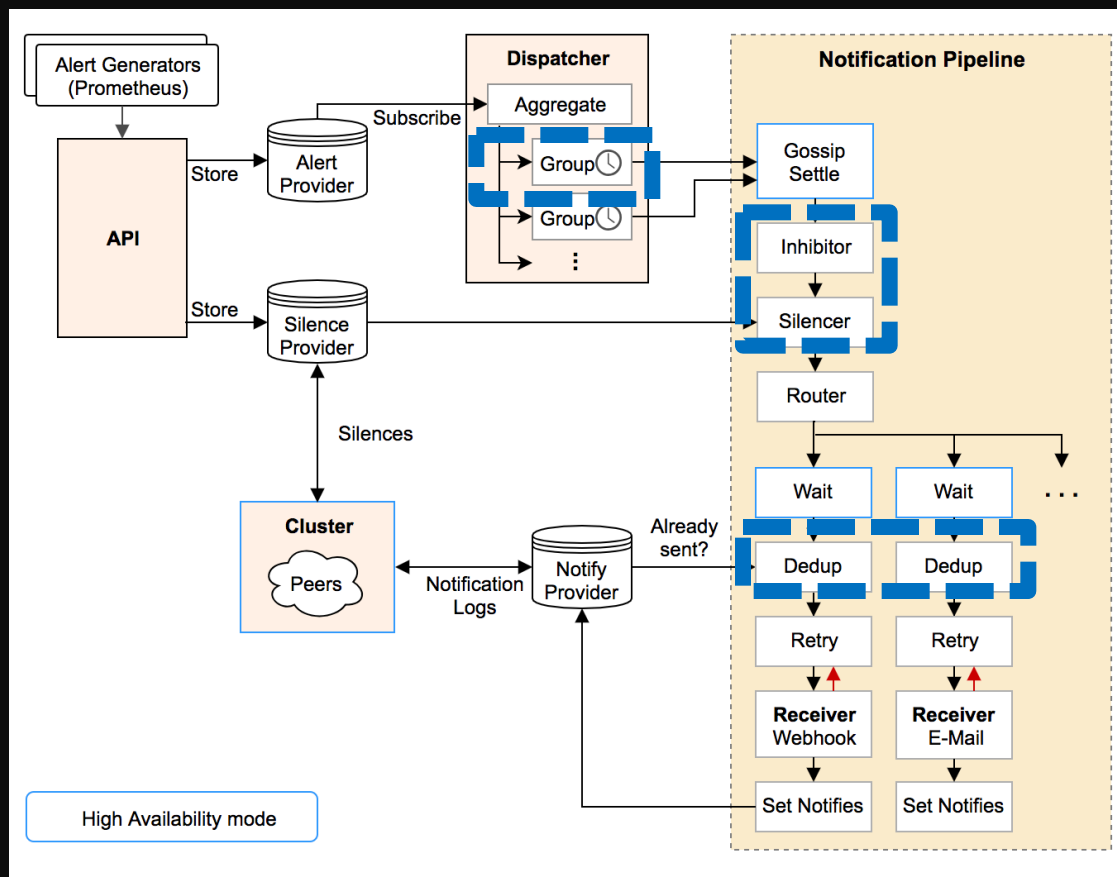
Alertmanager的实现

- 架 构
- 对 接
- 收 敛
- 配 置
- 可 用 性

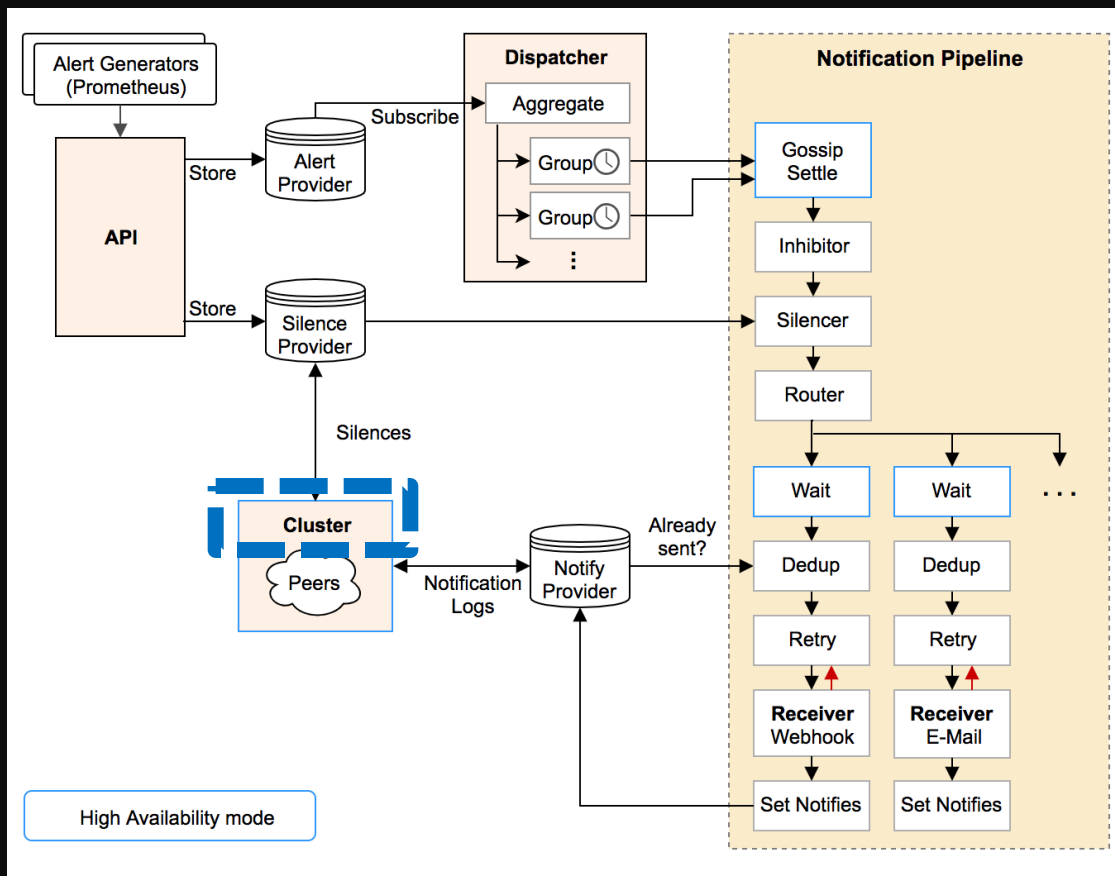
Alertmanager的实现-架构



Alertmanager的实现-架构



Alertmanager的实现-架构



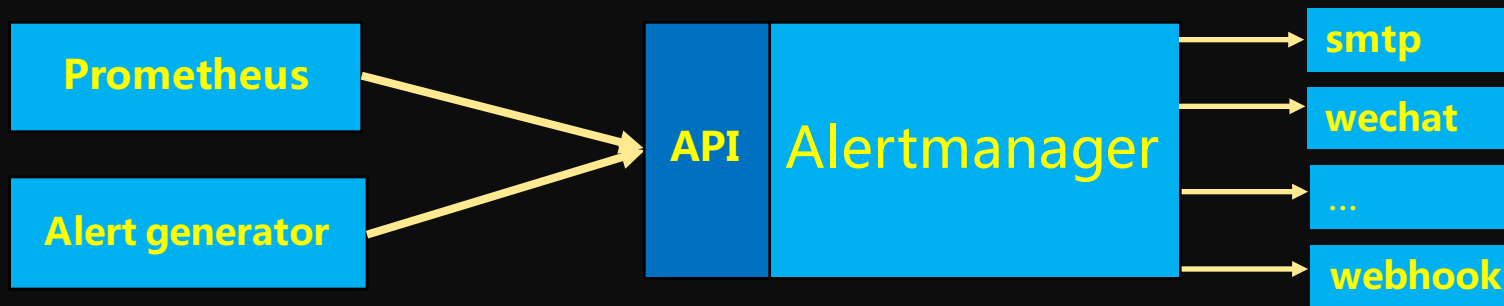
Alertmanager的实现

- 架 构
- 对 接
- 收 敛
- 配 置
- 可 用 性

Alertmanager的实现-对接

告警对接时需要满足什么要求？

- 接收不同告警源发送的告警
- 将不同的告警发往不同的接收者



Alertmanager的实现-对接

接收

HTTP API(/api/v1/alerts)

发送

The unique name of the receiver.

name: <string>

Configurations for several notification integrations.

email_configs: [- <email_config>, ...]

webhook_configs: [- <webhook_config>, ...]

wechat_configs: [- <wechat_config>, ...]

...

Alertmanager的实现

- 架 构
- 对 接
- 收 敛
- 配 置
- 可 用 性

Alertmanager的实现-收敛

- 分 组
- 抑 制
- 静 默
- 延 时

Alertmanager的实现-分组

- 减少告警消息的数量
- 同类告警的聚合帮助运维排查问题



Alertmanager的实现-分组

```
{alertname="mysql_cpu_high" id="mysql-A" }  
{alertname="mysql_uptime" id="mysql-B" }  
{alertname="mysql_slave_sql_thread_down" id="mysql-B"}  
{alertname="mysql_slave_io_thread_down" id="mysql-B"}
```



group_by: id

```
{alertname="mysql_cpu_high" id="mysql-A" }
```



```
{alertname="mysql_uptime" id="mysql-B" }  
{alertname="mysql_slave_sql_thread_down" id="mysql-B"}  
{alertname="mysql_slave_io_thread_down" id="mysql-B"}
```

Alertmanager的实现-收敛

- 分 组
- 抑 制
- 静 默
- 延 时

Alertmanager的实现-抑制

- 消除了冗余的告警



Alertmanager的实现-抑制

```
{alertname="mysql_uptime" server="server-A" }  
{alertname="server_uptime" server="server-A" }
```

server_uptime
抑制
mysql_uptime

```
{alertname="server_uptime" server="server-A" }
```

Alertmanager的实现-收敛

- 分 组
- 抑 制
- 静 默
- 延 时

Alertmanager的实现-静默

- 阻止发送可预期的告警

一堆的告警（实例1，实例2，实例3...）



静默实例1

一堆的告警（实例2，实例3...）

Alertmanager的实现-静默

```
{alertname="qps_more_than_3000" id="mysql-A" }  
{alertname="tps_more_than_2000" id="mysql-A" }  
{alertname="thread_running_more_than_200"  
id="mysql-A" }  
{alertname="thread_running_more_than_200"  
id="mysql-B" }
```



静默mysql-A的告警

```
{alertname="thread_running_more_than_20" id="mysql-B" }
```

Alertmanager的实现-收敛

- 分 组
- 抑 制
- 静 默
- 延 时

Alertmanager的实现-延时

- 不希望频繁的收到重复的告警消息怎么办？

Repeat interval

- 需要及时发送告警消息？

Group interval

- 故障刚发生时，接连收到几个告警消息怎么办？

Group wait

Alertmanager的实现

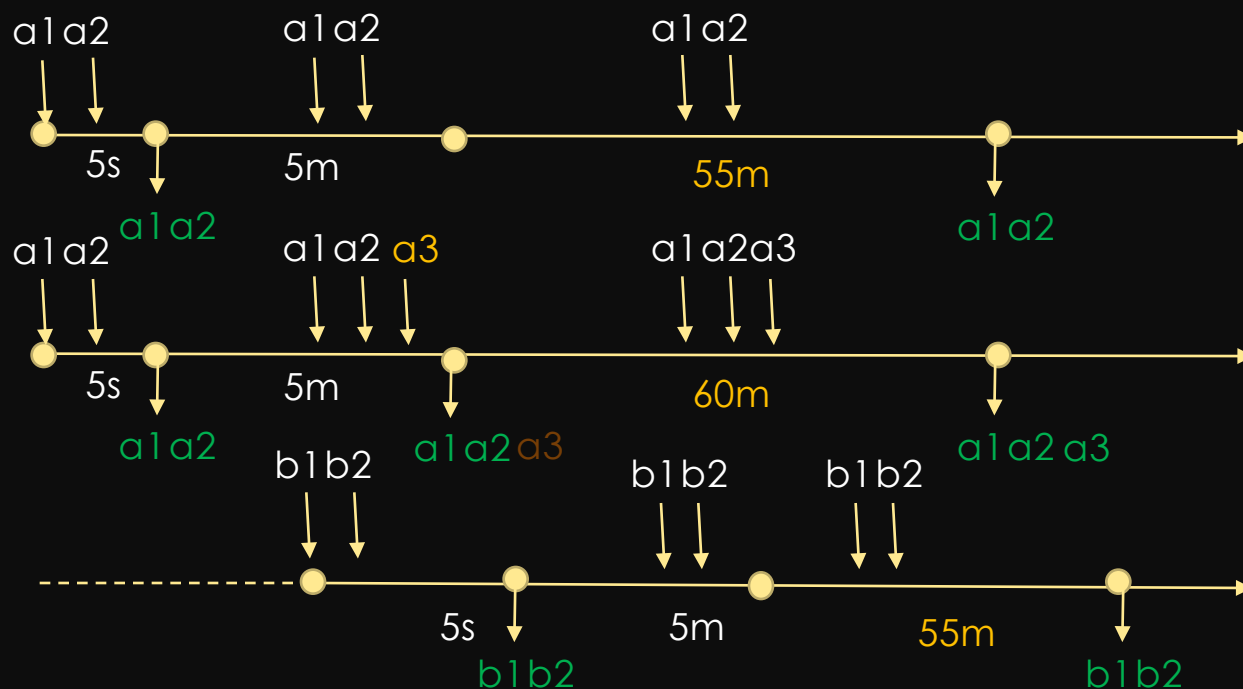
- 架 构
- 对 接
- 收 敛
- 配 置
- 可 用 性

Alertmanager的实现-告警收敛

分组A: a1, a2, a3

分组B: b1, b2

- Group wait: 5s
- Group interval: 5m
- Repeat interval: 60m



Alertmanager的实现-配置

- 使用**树形路由配置**，每个节点都定义了路由规则，匹配路由规则的告警都发往同一个接收者

匹配条件	接收者
id=~.+	默认负责人
id=~mongo-[a-zA-Z0-9]+	MongoDB运维
id=~mysql-[a-zA-Z0-9]+	MySQL运维
group=group1	业务1负责人
group=group2	业务2负责人

Alertmanager的实现-配置

route:

receiver: 'default-receiver'

group_wait: 5s

group_interval: 5m

repeat_interval: 1h

group_by: [db_type]

routes:

- **receiver:** 'mongo_ops_receiver'

group_wait: 10s

match_re:

service: mongo-[a-zA-Z0-9]+

- **receiver:** 'mysql_ops_receiver'

group_by: [mysql_id]

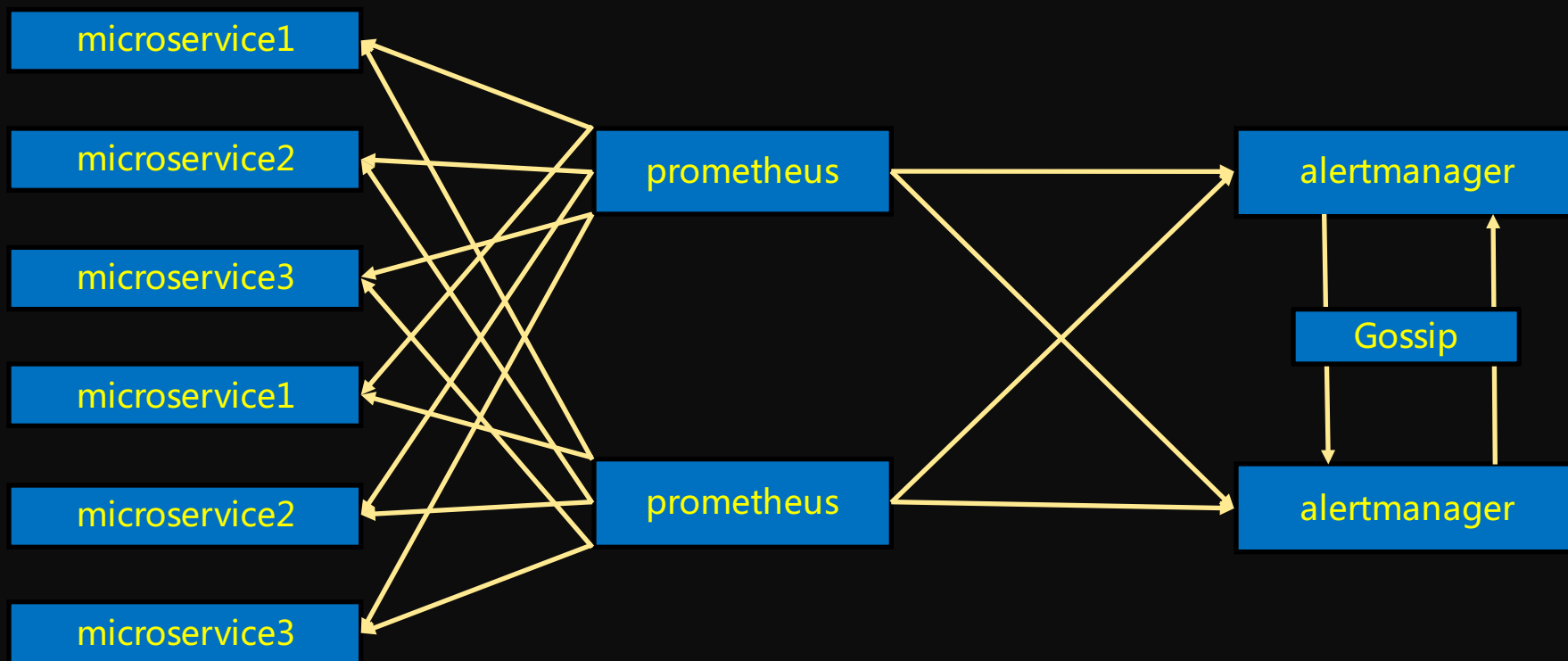
match:

group:group1

Alertmanager的实现

- 架 构
- 对 接
- 收 敛
- 配 置
- 可用 性

Alertmanager的实现-可用性



目录

CONTENTS

一.告警的选型

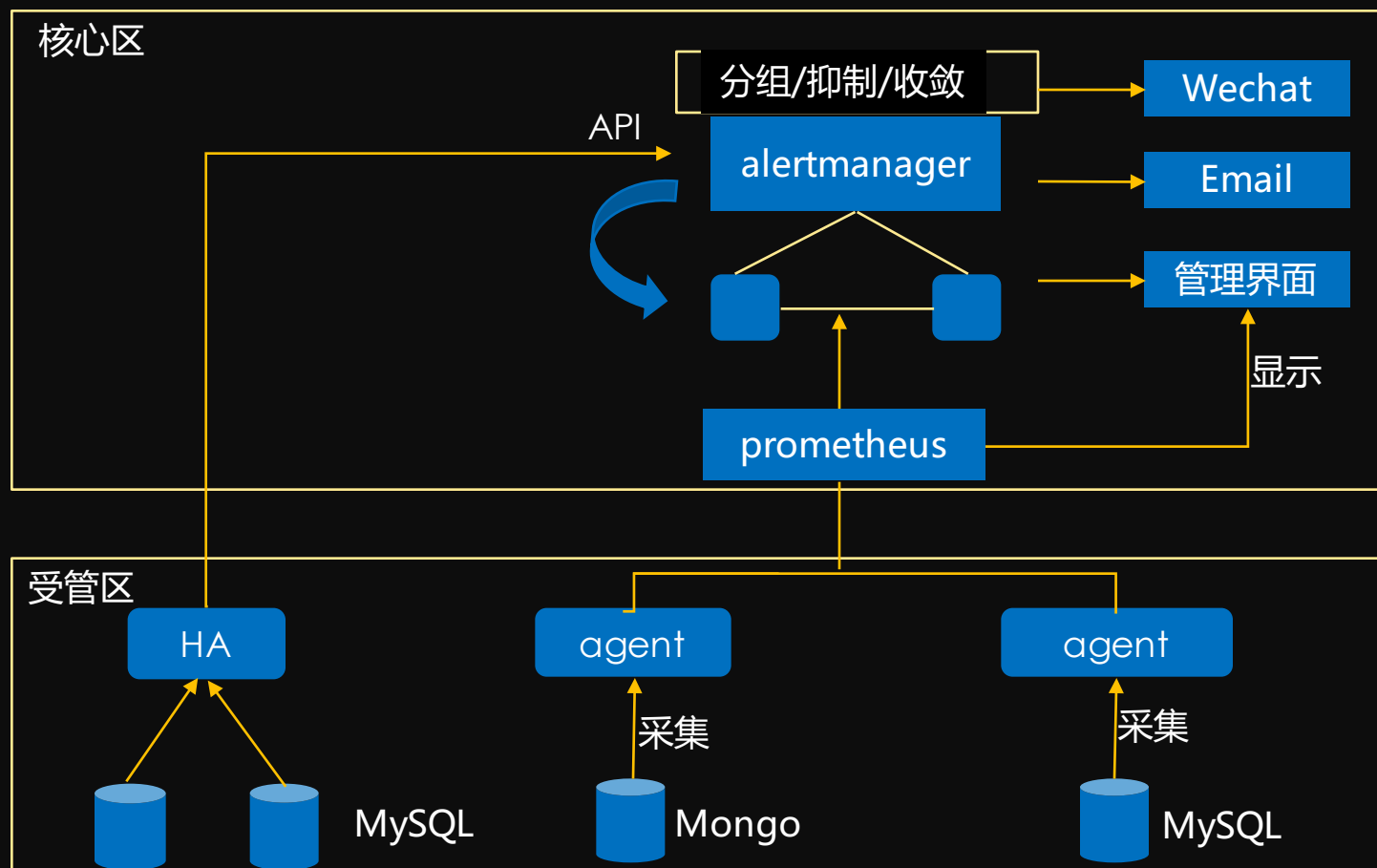
二.Alertmanager的实现

三.Alertmanager的实践

Alertmanager的实践

- 架 构
- 调度层级
- SRE

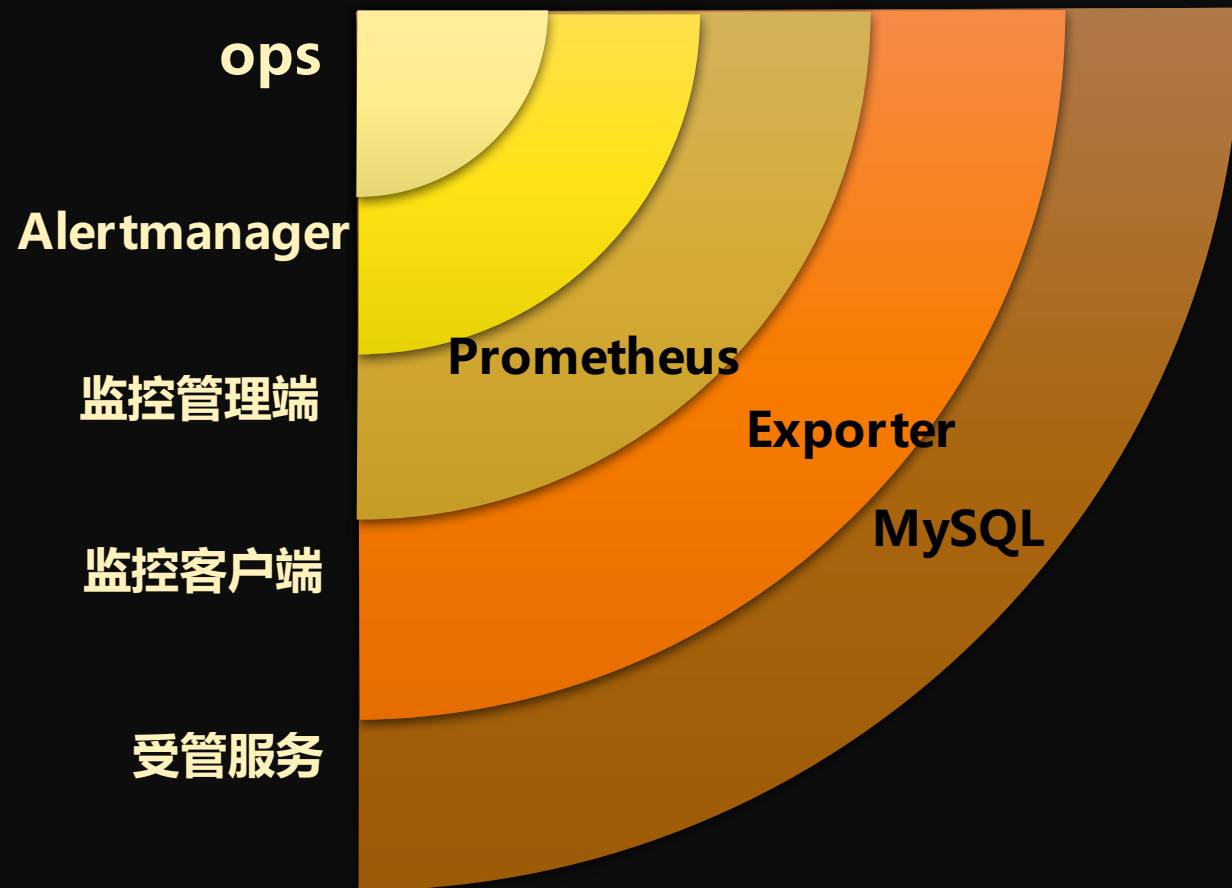
Alertmanager的实践-架构



Alertmanager的实践

- 架 构
- 调度层级
- SRE

Alertmanager的实践-调度层级



Alertmanager的实践

- 架 构
- 调度层级
- SRE

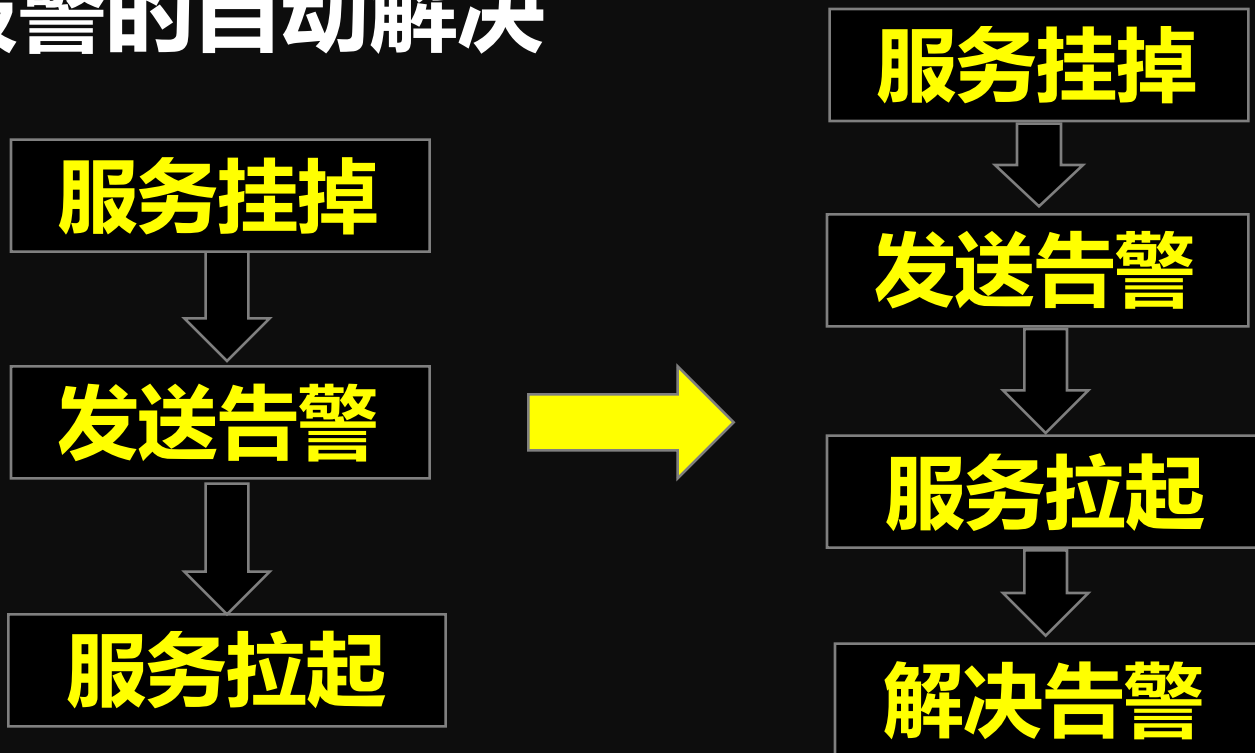
Alertmanager的实践-SRE

Google SRE 对监控系统的建议

- **报警**信息应由系统**自动解决**，仅当需要的时候才通知用户
- **收到报警**的用户需要**立即执行**某种**操作**，以解决已发生的问题或避免即将发生的问题

Alertmanager的实践-SRE

报警的自动解决



Alertmanager的实践-SRE

最大通知次数的限制



- 大规模集群告警经过Alertmanager收敛之后告警消息仍然可能很多
- 发送过多的相同的告警消息增加运维人员压力




Alertmanager的实践-SRE



发送NOTICE级别的告警

- 并不需要运维人员立即处理故障，只是作为一个通知消息



展示




 DMP  告警 | 阈值 设置 记录 测试

  admin 







 告警配置  提交告警设置修改


当前操作：暂无操作




 告警通道 

 添加告警通道  修改告警通道  移除告警通道



通道名	通道类型	通道描述
universe-null	null	
my_wechat	wechat	
my_smtp	wechat	



     





 告警抑制

 添加告警抑制  修改告警抑制  移除告警抑制



抑制分组标签	抑制源	抑制目标
alert_comp_id	code=mysql_replic_delay_more_than_1000	code=mysql_replic_delay_more_than_600
alert_comp_id	code=mysql_uptime	code=mysql_[a-zA-Z0-9_%]*
alert_comp_id	code=mysql_max_connections_more_than_80%	code=mysql_max_connections_more_than_60%


 




 告警配置 

 添加告警配置  添加告警配置子项  修改告警配置  移除告警配置



匹配条件	通道名	分组标签	分组报警时间(s)	命中后是否继续匹配?
<ul style="list-style-type: none">	universe-null	level	5 3600 300	false
<ul style="list-style-type: none">alert_comp_id=mysql-[a-zA-Z0-9]+	my_wechat	alert_comp_id	5 3600 300	true
<ul style="list-style-type: none">alert_comp_id=mysql-[a-zA-Z0-9]+	my_smtp	alert_comp_id	5 3600 300	false
<ul style="list-style-type: none">server=server-udp1	universe-null	alert_comp_id	5 3600 300	false

 告警静默

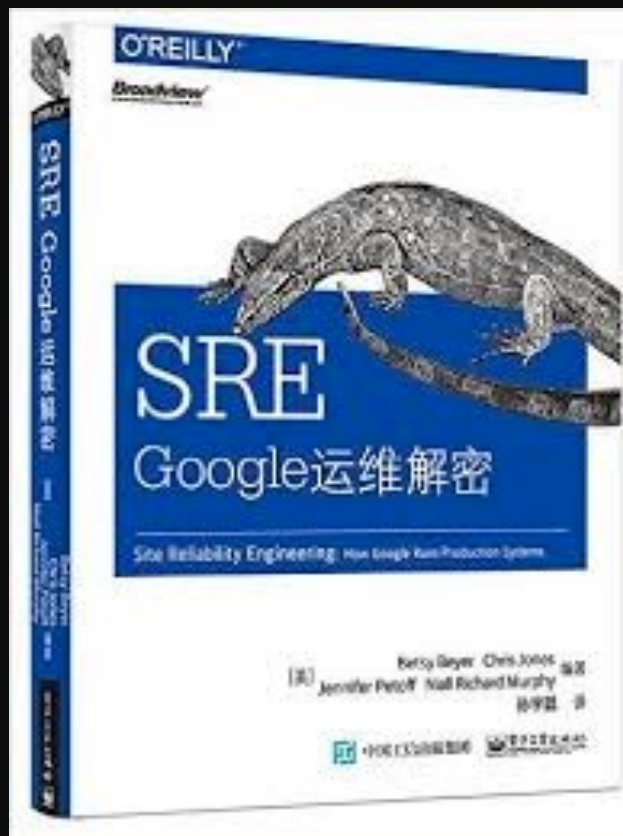
 添加告警静默  修改告警静默  移除告警静默

静默规则
server=server-udp3
alert_comp_id=mysql-93j9r1
code=test
level=NOTICE

DMP • 告警 • 设置

推荐





Thanks