# **Prometheus告警组件Alertmanager**

# **一、Alertmanager介绍**

实现Prometheus的告警，需Alertmanager这个组件。

Alertmanager与Prometheus是相互分离的两个组件。

所以，Alertmanager需单独安装配置。

通过在Prometheus中定义AlertRule（告警规则），Prometheus会周期性的对告警规则进行计算，

如果满足告警触发条件就会向Alertmanager发送告警信息。

在Prometheus中一条告警规则主要由告警名称和告警规则两部分组成：

* 告警名称：用户为告警规则命名
* 告警规则：告警规则由PromQL进行定义，其实际意义是当表达式（PromQL）查询结果持续多长时间（During）后出发告警，
Prometheus服务器根据报警规则将警报发送给Alertmanager，然后Alertmanager将静默（silencing）、抑制（inhibition）、分组聚合（aggregation）等消息通过Email、钉钉等发送通知。

Alertmanager特性

* 分组聚合：分组将同一类型的报警归类单个报警通知 。适用于当系统宕机导致大量报警被同时触发，此时分组机制可将这些被触发的告警合并为一个告警通知，避免一次性发送大量告警通知。
* 静默：提供了一个简单的机制可以快速根据标签对告警进行静默处理。特定时间不会发送告警通知。
* 抑制：指当警报发出后，停止重复发送由此警报引发其他错误的警报的机制。如网络不可达，导致其他服务连接相关警报。

# **二、Alertmanager安装及访问**

## 2.1 Alertmanager安装文件获取

[root@alertmanager ~]# wget https://github.com/prometheus/alertmanager/releases/download/v0.25.0/alertmanager-0.25.0.linux-amd64.tar.gz

[root@alertmanager ~]# tar xf alertmanager-0.25.0.linux-amd64.tar.gz
[root@alertmanager ~]# ls
alertmanager-0.25.0.linux-amd64

[root@alertmanager ~]# mv alertmanager-0.25.0.linux-amd64 /usr/local/alertmanager
[root@alertmanager ~]# cd /usr/local/alertmanager
[root@alertmanager alertmanager]# nohup /usr/local/alertmanager/alertmanager --config.file=/usr/local/alertmanager/alertmanager.yml &

[root@alertmanager alertmanager]# lsof -i tcp:9093
COMMAND PID USER FD TYPE DEVICE SIZE/OFF NODE NAME
alertmana 15889 root 8u IPv6 64844 0t0 TCP \*:copycat (LISTEN)

[root@alertmanager alertmanager]# ps -ef | grep alertmanager
root 15889 3381 0 18:09 pts/1 00:00:00 /usr/local/alertmanager/alertmanager --config.file=/usr/local/alertmanager/alertmanager.yml

可以把Alertmanager托管给systemd管理，示例如下：

[root@alertmanager alertmanager]# pkill alertmanager

注册为系统服务
[root@alertmanager alertmanager]# cat > /usr/lib/systemd/system/alertmanager.service << EOF
[Service]
ExecStart=/usr/local/alertmanager/alertmanager --config.file=/usr/local/alertmanager/alertmanager.yml

[Install]
WantedBy=multi-user.target

[Unit]
Description=alertmanager
After=network.target
EOF

重载/开机自启/查看状态/启动
[root@alertmanager alertmanager]# systemctl daemon-reload
[root@alertmanager alertmanager]# systemctl enable alertmanager

[root@alertmanager alertmanager]# systemctl start alertmanager

[root@alertmanager alertmanager]# systemctl status alertmanager

## 2.2 Alertmanager访问



# **三、Prometheus集成Alertmanager组件**

## 3.1 在Prometheus.yml文件中添加Alertmanager连接配置

[root@prometheus-server ~]# vim /usr/local/prometheus/prometheus.yml
 。。。
# Alertmanager configuration
alerting:
 alertmanagers:
 - static\_configs:
 - targets:
 - 192.168.10.17:9093 默认为# -alertmanager:9093,修改为alertmanager服务器IP地址+9093

## 3.2 在Prometheus.yml文件中添加告警规则配置文件位置

[root@prometheus-server ~]# vim /usr/local/prometheus/prometheus.yml

修改如下配置：
# Load rules once and periodically evaluate them according to the global 'evaluation\_interval'.
rule\_files:
 # - "first\_rules.yml"
 # - "second\_rules.yml"

为
# Load rules once and periodically evaluate them according to the global 'evaluation\_interval'.
rule\_files:
 - "rules/\*.yml"

rules为告警规则配置文件所在的目录，需要自行创建，创建位置为 /usr/local/prometheus/

[root@prometheus-server ~]# mkdir /usr/local/prometheus/rules

## 3.3 在Prometheus.yml文件中添加监控Alertmanager主机

为了对Alertmanager主机进行监控。

[root@prometheus-server ~]# vim /usr/local/prometheus/prometheus.yml

添加如下监控主机配置
scrape\_configs:
 ......
 - job\_name: "alertmanager"

 static\_configs:

 - targets: ["192.168.10.17:9093"]

## 3.4 重启Prometheus

[root@prometheus-server ~]# systemctl restart prometheus



# 四、配置alertmanager告警邮箱及告警规则（使用自己的邮箱）

## 4.1 配置alertmanager告警邮箱

在配置告警邮箱前，先配置邮箱授权码

[root@alertmanager alertmanager]# mv alertmanager.yml alertmanager.yml.bak

[root@alertmanager alertmanager]# vim alertmanager.yml
global:

 resolve\_timeout: 5m

 smtp\_smarthost: 'smtp.163.com:465'

 smtp\_from: 'wangliubao\_test@163.com'

 smtp\_auth\_username: 'wangliubao\_test@163.com'

 smtp\_auth\_password: 'MRIFLQVUNNGKLCOO'

 smtp\_require\_tls: false

 smtp\_hello: '163.com'

route:

 group\_by: ['alertname']

 group\_wait: 10s

 group\_interval: 5m

 repeat\_interval: 1m

 receiver: 'mail'

receivers:

 - name: 'mail'

 email\_configs:

 - to: 'wangliubao\_test@163.com'

[root@alertmanager alertmanager]# systemctl restart alertmanager
[root@alertmanager alertmanager]# systemctl status alertmanager

关于alertmanager.yaml文件的解释如下：
global: #全局设置，配置解决告警时间间隔和邮件发送服务
 resolve\_timeout: 5m # 定义持续多长时间未接收到告警标记后，就将告警状态标记为resolved
 smtp\_smarthost: 'smtp.126.com:465' # 邮件服务器
 smtp\_from: 'wangliubao\_test@163.com' # 发件人邮箱
 smtp\_auth\_username: '管理员邮箱' # 邮箱名
 smtp\_auth\_password: 'RXGFEHFQCLXAMFTP' # 邮箱认证使用授权码
 smtp\_require\_tls: false # 是否启动tls
route: # 路由树，每个告警都会在配置的顶级路由中进入路由树，路由树匹配所有报警规则
 group\_by: ['alertname'] # 告警过滤中分组标签
 group\_wait: 10s # 分组等待的时间
 group\_interval: 5m # 上下两组发送告警的间隔时间
 repeat\_interval: 1m # 重复发送告警时间，默认为1h,现修改为1分钟
 receiver: 'mail' # 指定告警媒介类型
receivers: # 告警接收器，这里配置接收邮箱地址。
- name: 'mail' # 告警来源自定义名称
 email\_configs:
 - to: '管理员邮箱' # 指定接收端email

## 4.2 配置alertmanager告警规则

[root@prometheus-server ~]# mkdir /usr/local/prometheus/rules

[root@prometheus-server ~]# cat /usr/local/prometheus/rules/node\_alerts.yml
groups:
- name: general.rules
 rules:
 - alert: NodeFilesystemUsage
 expr: 100 - (node\_filesystem\_free\_bytes{mountpoint="/",fstype=~"ext4|xfs"} / node\_filesystem\_size\_bytes{fstype=~"ext4|xfs"} \* 100) > 30
 for: 1m
 labels:
 severity: warning
 annotations:
 summary: "Instance {{ $labels.instance }} : {{ $labels.mountpoint }} 分区使用率过高"
 description: "{{ $labels.instance }} : {{ $labels.job }} : {{$labels.mountpoint}} 这个分区使用大于百分之30% (当前值: {{ $value }})"

[root@prometheus-server ~]# systemctl restart prometheus
[root@prometheus-server ~]# systemctl status prometheus

关于告警规则的解析说明如下：
groups:
- name: general.rules # 告警规则组名称
 rules: # 定义规则
 - alert: NodeFilesystemUsage # 告警名称，在Alertmanager及邮箱可见。
 expr: 100 - (node\_filesystem\_free\_bytes{mountpoint="/",fstype=~"ext4|xfs"} / node\_filesystem\_size\_bytes{fstype=~"ext4|xfs"} \* 100) > 30 # 表达式，获取硬盘使用率 大于30% 触发告警
 for: 1m # 持续时间，表示持续1分钟获取不到信息，则触发报警，0表示不使用持续时间。
 labels: # 定义当前告警规则级别
 severity: warning
 annotations: #注释 告警通知
 summary: "Instance {{ $labels.instance }} : {{ $labels.mountpoint }} 分区使用率过高"
 description: "{{ $labels.instance }} : {{ $labels.job }} : {{$labels.mountpoint}} 这个分区使用大于百分之30% (当前值: {{ $value }})"
 # 调用标签具体附加通知信息，在邮件中可见

在192.168.10.14主机上使用命令创建占用磁盘空间的大文件，以达到测试的目的。
dd if=/dev/zero of=/test bs=1M count=20000

在192.168.10.15主机上使用命令创建占用磁盘空间的大文件，以达到测试的目的。
dd if=/dev/zero of=/test bs=1M count=20000











Prometheus主机alerts显示告警信息

