背景

在《Prometheus监控实战》这本书中，我们知道⼀个良好的监控系统应该满⾜/提供以下内容：

全局视⻆，从最⾼层(业务)依次展开；协助故障诊断；

作为基础设施、应⽤程序开发和业务⼈员的信息源；内置于应⽤程序设计、开发和部署的⽣命周期中； 尽可能的⾃动化，并提供⾃服务；

拥有了⼀个良好的监控系统之后，这还不够。我们还需要⼀个告警消息，告警消息可以为我们体统⼀些指示，表明我们环境中的某些状态已经发⽣了变化，⽽且通常是⼀些更糟糕的情况，⼀个好的告警消息的关键应该是能够在正确的时间，以正确的理由和正确的速度发送，并且其中包含了有⽤的信息；

那么告警消息的发送的⽬的地，也成为了其中关键的⼀个环节，从传统的E-mail、电话、短信通知到现在层出不穷的企业办公聊天软件，如钉钉、企业微信、⻜书等，选择合适的⼯具来接收通知，以保证处理⼈员能够及时的收到消息尤为重要；

以SUSE Rancher企业版为例，其中集成了除E-mail、slack等常⽤的通知平台外，还特别针对中国企业

⽤户集成了钉钉、企业微信、阿⾥云短信等通知平台，但是即使是这样，在某些企业⽤户的⻆度仍然⽆法满

⾜其需求，⽐如说⻜书⽤户，就没办法直接进⾏对接。在本⽂中，使⽤SUSE Rancher告警通知中的Webhook

⽅式结合另⼀个优秀的开源项⽬PrometheusAlert实现多种通知平台的告警发送；

PrometheusAlert全家桶

\*PrometheusAlert是开源的运维告警中⼼消息转发系统，⽀持主流的监控系统Prometheus、Zabbix，

⽇志系统Graylog2，Graylog3、数据可视化系统Grafana、SonarQube。阿⾥云-云监控，以及所有⽀持WebHook接⼝的系统发出的预警消息，⽀持将收到的这些消息发送到钉钉，微信，email，⻜书，腾讯短信，腾讯电话，阿⾥云短信，阿⾥云电话，华为短信，百度云短信，容联云电话，七陌短信，七陌语⾳，TeleGram，百度Hi(如流)等。

以上内容引⽤PrometheusAlert项⽬简介，可以看到这个项⽬可以对接多种的主流监控系统，并且⽀持通过webhook接⼝发送的告警消息，推送到多种接受平台。并且项⽬处于活跃状态，在进⾏不断更新，未来会有更多的平台接⼊，感兴趣的同学可以查看并参与其中。

项⽬地址：https://github.com/feiyu563/PrometheusAlert

让告警⻜起来

本⽂中将使⽤SUSE Rancher和PrometheusAlert实现SUSE Rancher产⽣的告警通知发送到⻜书中进⾏演示，更多配置可以查看PrometheusAlert项⽬⽂档；

创建⻜书机器⼈

创建⼀个⻜书群组，并添加⼀个⾃定义机器⼈；

记录⽣成的webhook地址；这⼀步可以根据需求定义安全相关配置；



更多关于⻜书机器⼈请查看链接：

https://open.feishu.cn/document/ukTMukTMukTM/ucTM5YjL3ETO24yNxkjN

# 部署PrometheusAlert

本⽂中将PrometheusAlert部署在SUSE Rancher创建的⾃定kubernetes集群中，使⽤yaml⽂件进⾏部

署；

创建Configmap

这⼀步骤中创建PrometheusAlert的Configmap配置，PrometheusAlert也提供了通过环境变量的⽅式注

⼊配置，但是为了⽅便管理，这⾥使⽤Configmap的⽅式；

apiVersion: v1 data:

app.conf: |-

#---------------------↓全局配置-----------------------

appname = PrometheusAlert #登录⽤户名

login\_user=prometheusalert #登录密码

login\_password=prometheusalert #监听地址

httpaddr = "0.0.0.0" #监听端⼝

httpport = 8080 runmode = dev

#设置代理 proxy = http://123.123.123.123:8080

proxy =

#开启JSON请求

copyrequestbody = true #告警消息标题

title=PrometheusAlert #链接到告警平台地址

[GraylogAlerturl=http://graylog.org](http://graylog.org/) #钉钉告警 告警logo图标地址

logourl=https://raw.githubusercontent.com/feiyu563/PrometheusAlert/master/ doc/alert-center.png

#钉钉告警 恢复logo图标地址

rlogourl=https://raw.githubusercontent.com/feiyu563/PrometheusAlert/master

/doc/alert-center.png

#短信告警级别(等于3就进⾏短信告警) 告警级别定义 0 信息,1 警告,2 ⼀般严重,3 严重,4

灾难

messagelevel=3

#电话告警级别(等于4就进⾏语⾳告警) 告警级别定义 0 信息,1 警告,2 ⼀般严重,3 严重,4

灾难

phonecalllevel=4

#默认拨打号码(⻚⾯测试短信和电话功能需要配置此项)

defaultphone=xxxxxxxx

#故障恢复是否启⽤电话通知0为关闭,1为开启

phonecallresolved=0

#是否前台输出file or console

logtype=file #⽇志⽂件路径

logpath=logs/prometheusalertcenter.log

#转换Prometheus,graylog告警消息的时区为CST时区(如默认已经是CST时区，请勿开启)

prometheus\_cst\_time=0

#数据库驱动，⽀持sqlite3，mysql,postgres如使⽤mysql或postgres，请开启 db\_host,db\_port,db\_user,db\_password,db\_name的注释

db\_driver=sqlite3 #db\_host=127.0.0.1 #db\_port=3306 #db\_user=root #db\_password=root #db\_name=prometheusalert

#是否开启告警记录 0为关闭,1为开启

AlertRecord=0

#是否开启告警记录定时删除 0为关闭,1为开启

RecordLive=0

#告警记录定时删除周期，单位天

RecordLiveDay=7

# 是否将告警记录写⼊es7，0为关闭，1为开启

alert\_to\_es=0

# es地址，是[]string

# beego.Appconfig.Strings读取配置为[]string，使⽤";"⽽不是","

to\_es\_url=http://localhost:9200

# to\_es\_url=http://es1:9200;http://es2:9200;http://es3:9200 # es⽤户和密码

# to\_es\_user=username # to\_es\_pwd=password

#---------------------↓webhook-----------------------

#是否开启钉钉告警通道,可同时开始多个通道0为关闭,1为开启

open-dingding=1 #默认钉钉机器⼈地址

ddurl=https://oapi.dingtalk.com/robot/send?access\_token=xxxxx #是否开启 @所有⼈(0为关闭,1为开启)

dd\_isatall=1

#是否开启微信告警通道,可同时开始多个通道0为关闭,1为开启 open-weixin=1

#默认企业微信机器⼈地址

wxurl=https://qyapi.weixin.qq.com/cgi-bin/webhook/send?key=xxxxx

#是否开启⻜书告警通道,可同时开始多个通道0为关闭,1为开启 open-feishu=0

#默认⻜书机器⼈地址

fsurl=https://open.feishu.cn/open-apis/bot/hook/xxxxxxxxx

#---------------------↓腾讯云接⼝-----------------------

#是否开启腾讯云短信告警通道,可同时开始多个通道0为关闭,1为开启

open-txdx=0

#腾讯云短信接⼝key

TXY\_DX\_appkey=xxxxx

#腾讯云短信模版ID 腾讯云短信模版配置可参考 prometheus告警:{1}

TXY\_DX\_tpl\_id=xxxxx #腾讯云短信sdk app id

TXY\_DX\_sdkappid=xxxxx

#腾讯云短信签名 根据⾃⼰审核通过的签名来填写

TXY\_DX\_sign=腾讯云

#是否开启腾讯云电话告警通道,可同时开始多个通道0为关闭,1为开启 open-txdh=0

#腾讯云电话接⼝key

TXY\_DH\_phonecallappkey=xxxxx #腾讯云电话模版ID

TXY\_DH\_phonecalltpl\_id=xxxxx #腾讯云电话sdk app id

TXY\_DH\_phonecallsdkappid=xxxxx

#---------------------↓华为云接⼝-----------------------

#是否开启华为云短信告警通道,可同时开始多个通道0为关闭,1为开启

open-hwdx=0

#华为云短信接⼝key

HWY\_DX\_APP\_Key=xxxxxxxxxxxxxxxxxxxxxx #华为云短信接⼝Secret

HWY\_DX\_APP\_Secret=xxxxxxxxxxxxxxxxxxxxxx #华为云APP接⼊地址(端⼝接⼝地址)

HWY\_DX\_APP\_Url=https://rtcsms.cn-north-1.myhuaweicloud.com:10743 #华为云短信模板ID

HWY\_DX\_Templateid=xxxxxxxxxxxxxxxxxxxxxx

#华为云签名名称，必须是已审核通过的，与模板类型⼀致的签名名称,按照⾃⼰的实际签名填写 HWY\_DX\_Signature=华为云

#华为云签名通道号

HWY\_DX\_Sender=xxxxxxxxxx

#---------------------↓阿⾥云接⼝-----------------------

#是否开启阿⾥云短信告警通道,可同时开始多个通道0为关闭,1为开启

open-alydx=0

#阿⾥云短信主账号AccessKey的ID

ALY\_DX\_AccessKeyId=xxxxxxxxxxxxxxxxxxxxxx #阿⾥云短信接⼝密钥

ALY\_DX\_AccessSecret=xxxxxxxxxxxxxxxxxxxxxx #阿⾥云短信签名名称

ALY\_DX\_SignName=阿⾥云 #阿⾥云短信模板ID

ALY\_DX\_Template=xxxxxxxxxxxxxxxxxxxxxx

#是否开启阿⾥云电话告警通道,可同时开始多个通道0为关闭,1为开启 open-alydh=0

#阿⾥云电话主账号AccessKey的ID

ALY\_DH\_AccessKeyId=xxxxxxxxxxxxxxxxxxxxxx #阿⾥云电话接⼝密钥

ALY\_DH\_AccessSecret=xxxxxxxxxxxxxxxxxxxxxx #阿⾥云电话被叫显号，必须是已购买的号码

ALY\_DX\_CalledShowNumber=xxxxxxxxx #阿⾥云电话⽂本转语⾳（TTS）模板ID

ALY\_DH\_TtsCode=xxxxxxxx

#---------------------↓容联云接⼝-----------------------

#是否开启容联云电话告警通道,可同时开始多个通道0为关闭,1为开启

open-rlydh=0

#容联云基础接⼝地址

RLY\_URL=https://app.cloopen.com:8883/2013-12-26/Accounts/ #容联云后台SID

RLY\_ACCOUNT\_SID=xxxxxxxxxxx #容联云api-token

RLY\_ACCOUNT\_TOKEN=xxxxxxxxxx #容联云app\_id

RLY\_APP\_ID=xxxxxxxxxxxxx

#---------------------↓邮件配置-----------------------

#是否开启邮件

open-email=0

#邮件发件服务器地址

Email\_host=smtp.qq.com #邮件发件服务器端⼝

Email\_port=465 #邮件帐号

[Email\_user=xxxxxxx@qq.com](mailto:Email_user%3Dxxxxxxx@qq.com) #邮件密码

Email\_password=xxxxxx #邮件标题

Email\_title=运维告警 #默认发送邮箱

Default\_emails=xxxxx@qq.com,xxxxx@qq.com

#---------------------↓七陌云接⼝-----------------------

#是否开启七陌短信告警通道,可同时开始多个通道0为关闭,1为开启

open-7moordx=0 #七陌账户ID

7MOOR\_ACCOUNT\_ID=Nxxx

#七陌账户APISecret

7MOOR\_ACCOUNT\_APISECRET=xxx

#七陌账户短信模板编号

7MOOR\_DX\_TEMPLATENUM=n

#注意：七陌短信变量这⾥只⽤⼀个var1，在代码⾥写死了。

#-----------

#是否开启七陌webcall语⾳通知告警通道,可同时开始多个通道0为关闭,1为开启

open-7moordh=0

#请在七陌平台添加虚拟服务号、⽂本节点 #七陌账户webcall的虚拟服务号

7MOOR\_WEBCALL\_SERVICENO=xxx

# ⽂本节点⾥被替换的变量，我配置的是text。如果被替换的变量不是text，请修改此配置

7MOOR\_WEBCALL\_VOICE\_VAR=text

#---------------------↓telegram接⼝-----------------------

#是否开启telegram告警通道,可同时开始多个通道0为关闭,1为开启

open-tg=0 #tg机器⼈token

TG\_TOKEN=xxxxx

#tg消息模式 个⼈消息或者频道消息 0为关闭(推送给个⼈)，1为开启(推送给频道)

TG\_MODE\_CHAN=0

#tg⽤户ID

TG\_USERID=xxxxx

#tg频道name或者id, 频道name需要以@开始

TG\_CHANNAME=xxxxx

#tg api地址, 可以配置为代理地址

#TG\_API\_PROXY="https://api.telegram.org/bot%s/%s"

#---------------------↓workwechat接⼝-----------------------

#是否开启workwechat告警通道,可同时开始多个通道0为关闭,1为开启

open-workwechat=0 # 企业ID

WorkWechat\_CropID=xxxxx # 应⽤ID

WorkWechat\_AgentID=xxxx # 应⽤secret

WorkWechat\_AgentSecret=xxxx # 接受⽤户

WorkWechat\_ToUser="zhangsan|lisi" # 接受部⻔

WorkWechat\_ToParty="ops|dev" # 接受标签

WorkWechat\_ToTag=""

# 消息类型, 暂时只⽀持markdown

# WorkWechat\_Msgtype = "markdown"

#---------------------↓百度云接⼝-----------------------

#是否开启百度云短信告警通道,可同时开始多个通道0为关闭,1为开启

open-baidudx=0

#百度云短信接⼝AK(ACCESS\_KEY\_ID)

BDY\_DX\_AK=xxxxx

#百度云短信接⼝SK(SECRET\_ACCESS\_KEY)

BDY\_DX\_SK=xxxxx

#百度云短信ENDPOINT（ENDPOINT参数需要⽤指定区域的域名来进⾏定义，如服务所在区域为北京，则为）

[BDY\_DX\_ENDPOINT=http://smsv3.bj.baidubce.com](http://smsv3.bj.baidubce.com/)

#百度云短信模版ID,根据⾃⼰审核通过的模版来填写(模版⽀持⼀个参数code：如prometheus

告警:{code})

BDY\_DX\_TEMPLATE\_ID=xxxxx

#百度云短信签名ID，根据⾃⼰审核通过的签名来填写

TXY\_DX\_SIGNATURE\_ID=xxxxx

#---------------------↓百度Hi(如流)-----------------------

#是否开启百度Hi(如流)告警通道,可同时开始多个通道0为关闭,1为开启

open-ruliu=0

#默认百度Hi(如流)机器⼈地址

BDRL\_URL=https://api.im.baidu.com/api/msg/groupmsgsend? access\_token=xxxxxxxxxxxxxx

#百度Hi(如流)群ID

BDRL\_ID=123456

#---------------------↓bark接⼝-----------------------

#是否开启telegram告警通道,可同时开始多个通道0为关闭,1为开启

open-bark=0

#bark默认地址, 建议⾃⾏部署bark-server

BARK\_URL=https://api.day.app #bark key, 多个key使⽤分割

BARK\_KEYS=xxxxx # 复制, 推荐开启

BARK\_COPY=1

# 历史记录保存,推荐开启

BARK\_ARCHIVE=1

# 消息分组

BARK\_GROUP=PrometheusAlert kind: ConfigMap

metadata:

name: prometheus-alert-center-conf namespace: kube-system

根据实际需要进⾏配置⽂件的修改，这⾥我们对接⻜书，主要有以下⼏个参数需要修改

login\_user=prometheusalert ## UI登陆⽤户名 login\_password=prometheusalert ##UI登陆密码 open-feishu=1 ##修改为1，启⽤⻜书告警

fsurl=https://open.feishu.cn/open-apis/bot/hook/xxxxxxxxx ##⻜书机器⼈ webhook地址(也可以在后续⻚⾯中填写)

部署⼯作负载

通过yaml部署PrometheusAlert⼯作负载和Nodeport类型的Service以⽤于访问PrometheusAlert UI(SUSE Rancher UI可以直接导⼊);

apiVersion: apps/v1 kind: Deployment metadata:

labels:

app: prometheus-alert-center alertname: prometheus-alert-center

name: prometheus-alert-center namespace: kube-system

spec:

replicas: 1 selector:

matchLabels:

app: prometheus-alert-center alertname: prometheus-alert-center

strategy: rollingUpdate:

maxSurge: 1

maxUnavailable: 0 type: RollingUpdate

template: metadata:

labels:

app: prometheus-alert-center alertname: prometheus-alert-center

spec:

containers:

---

* env:

- name: TZ

value: Asia/Shanghai

image: feiyu563/prometheus-alert imagePullPolicy: IfNotPresent name: prometheus-alert-center resources:

limits: cpu: 500m

memory: 512Mi requests:

cpu: 200m memory: 128Mi

volumeMounts:

- mountPath: /app/conf/ name: vol1

dnsPolicy: ClusterFirst restartPolicy: Always schedulerName: default-scheduler securityContext: {} terminationGracePeriodSeconds: 30 volumes:

* configMap:

defaultMode: 256

name: prometheus-alert-center-conf optional: false

name: vol1

apiVersion: v1 kind: Service metadata:

name: prometheus-alert-center namespace: kube-system

spec:

type: NodePort selector:

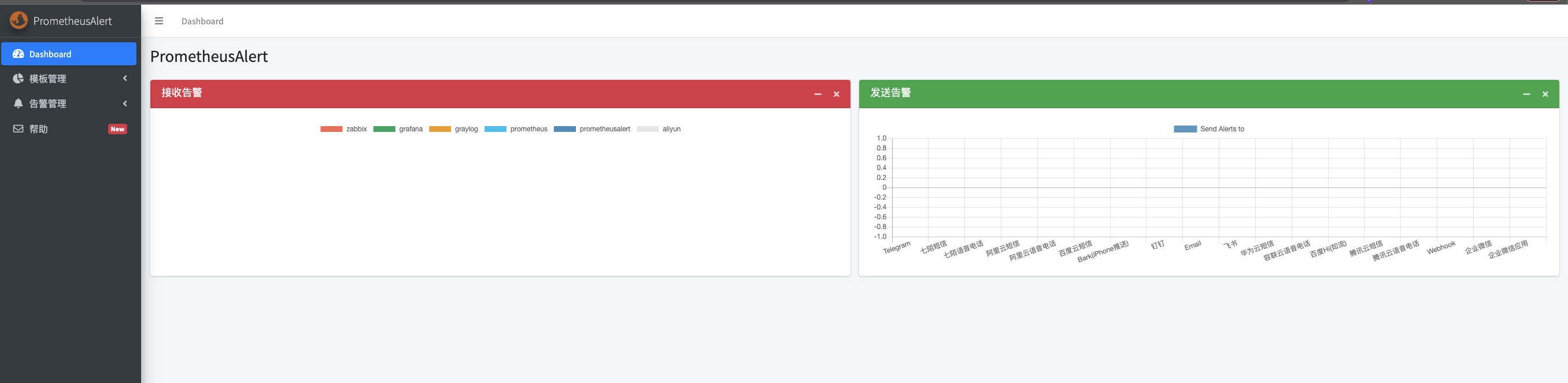
app: prometheus-alert-center ports:

- port: 8080

targetPort: 8080

nodePort: 30080

部署完成后通过访问http://<node\_ip>:30080即可访问PrometheusAlert UI，⽤户名和密码为 Configmap中的配置；⾄此，PrometheusAlert全家桶部署完毕，除了以上基础配置以外 PrometheusAlert全家桶还有更多的部署⽅式和配置，⽐如说使⽤后端mysql存储进⾏模版的存储等，更多部署细节可以查看项⽬⽂档链接：https://feiyu563.gitbook.io/prometheusalert/base-install



创建⾃定义告警模版

PrometheusAlert全家桶部署完成后，因为使⽤SUSE Rancher通知发送出去的Webhook消息与原⽣的有所不同，因此我们需要添加PrometheusAlert全家桶中的⾃定义告警模版；

注意：SUSE Rancher告警通知模版和PrometheusAlert全家桶⾃定义模版需要有⼀定的Go

template 基础；；

添加⾃定义PrometheusAlert告警模版

在PrometheusAlert全家桶中添加⾃定义模版，以下内容为必填项

模版名称模版类型模版内容模版⽤途

这⾥我们选择模版类型为⻜书，模版⽤途为Prometheus，模版内容如下

{{ $var := .externalURL}}{{ range $k,$v:=.alerts }}

{{if eq $v.status "resolved"}}

\*\*[Rancher容器云平台恢复告警信息]({{$v.labels.server\_url}})\*\*

\*[{{$v.labels.alertname}}]({{$var}})\*

告警级别：{{$v.labels.severity}}

开始时间：{{TimeFormat $v.startsAt "2006-01-02 15:04:05 UTC"}}

结束时间：{{TimeFormat $v.endsAt "2006-01-02 15:04:05 UTC"}}

集群ID: {{$v.labels.cluster\_name}}

故障主机IP: {{$v.labels.instance}}

PromQL: {{$v.alert.expression}}

触发告警持续时间: {{$v.labels.duration}}

当前值为：\*\*{{$v.annotations.current\_value}}\*\*

{{else}}

\*\*[Rancher容器云平台告警信息]({{$v.labels.server\_url}})\*\*

\*[{{$v.labels.alertname}}]({{$var}})\*

告警级别：{{$v.labels.severity}}

开始时间：{{TimeFormat $v.startsAt "2006-01-02 15:04:05 UTC"}}

{{if eq $v.endsAt "0001-01-01T00:00:00Z"}}

结束时间: {{ printf "告警当前仍然存在!"}}

{{else}}

结束时间: {{TimeFormat $v.endsAt "2006-01-02 15:04:05 UTC"}}

{{end}}

集群ID: {{$v.labels.cluster\_name}}

故障主机IP: {{$v.labels.instance}}

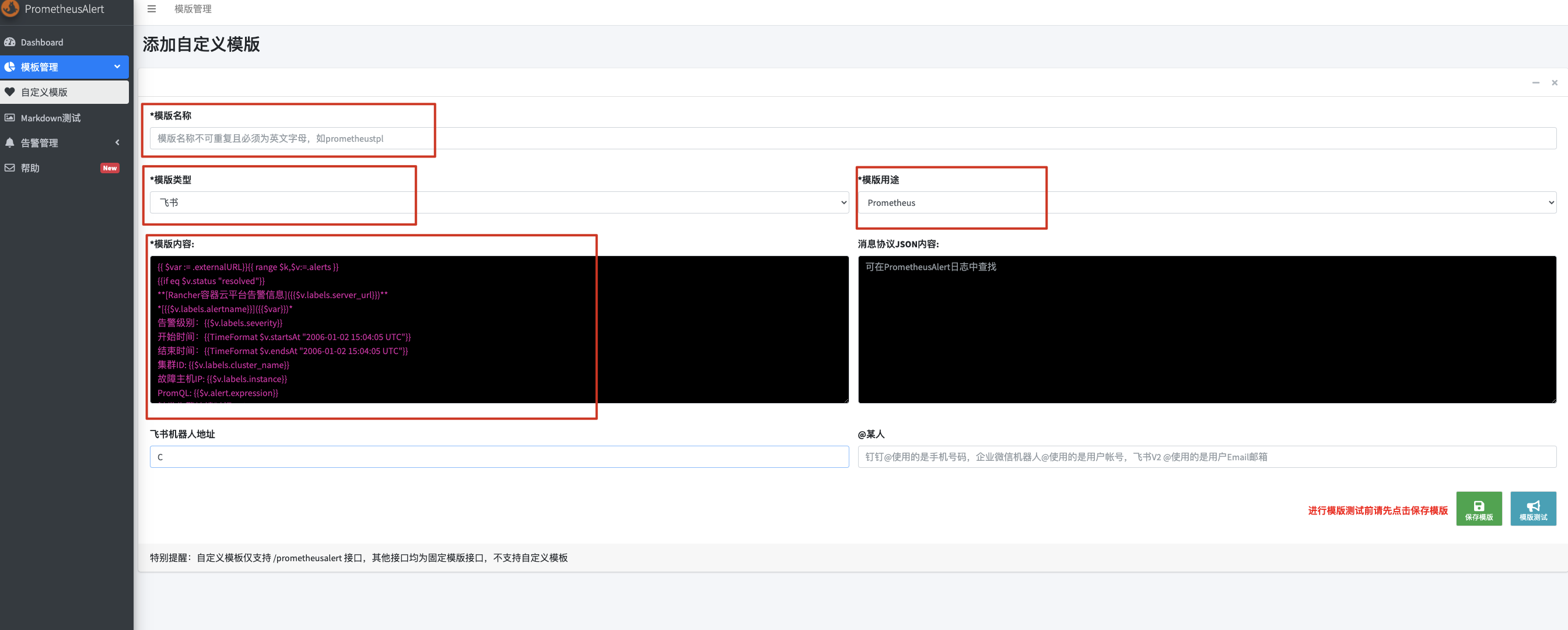
PromQL: {{$v.labels.expression}}

触发告警持续时间: {{$v.labels.duration}}

当前值为：\*\*{{$v.annotations.current\_value}}\*\*

{{end}}

{{ end }}



这⾥的模版内容均为go template编写，在本⽂中仅以SUSE Rancher发出的默认webhook消息作

为示例，对于有go template基础或者SUSE Rancher使⽤基础的⽤户，可以基于SUSE Rancher企业版的⾃定义告警功能和⾃定义告警通知模版功能对告警消息进⾏深度定制，然后在 PrometheusAlert全家桶⾃定义模版中定义更⾼级的告警消息；

SUSE Rancher告警对接

⾸先在集群/项⽬--⼯具--通知中添加Webhook类型的通知，URL填写如下：

http://<PrometheusAlert\_url>/prometheusalert? type=fs&tpl=RancherTofs&fsurl=https://open.feishu.cn/open- apis/bot/v2/hook/xxxxxxxxx

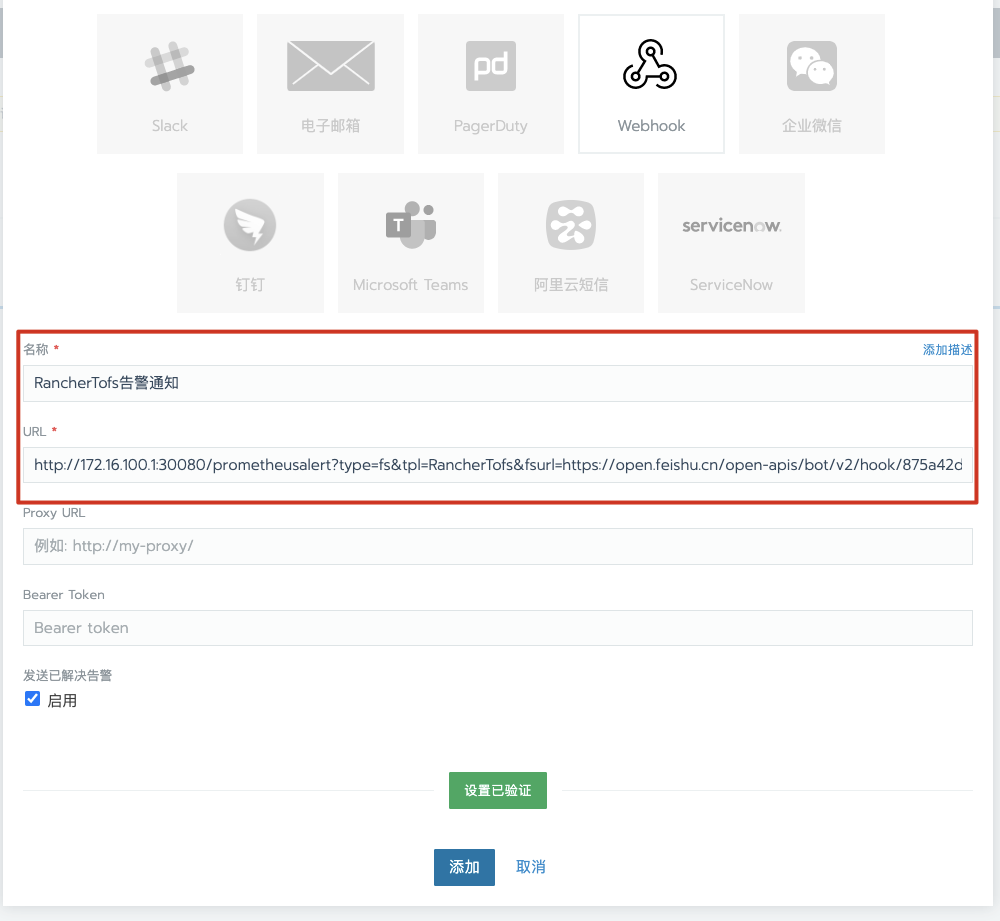
<PrometheusAlert\_url> PrometheusAlert地址 typt=fs 类型为⻜书

tpl=RancherTofs 上⼀步创建的PrometheusAlert模版名称

fsurl ⻜书机器⼈的webhook地址

PrometheusAlert有⾃⼰的接⼝格式，更多接⼝细节请参考PrometheusAlert⽂档，本⽂仅以⻜

书举例；



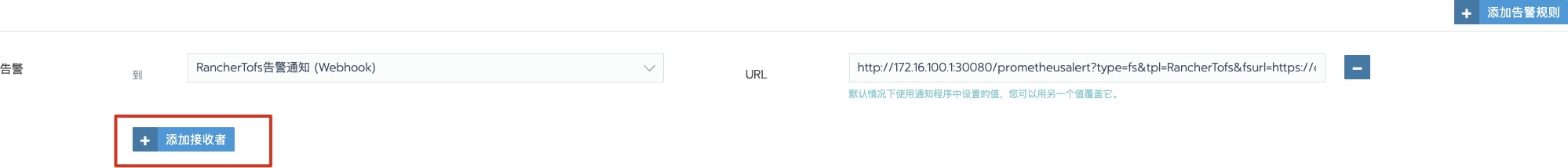
这⾥需要注意的是，与以往的对接⽅式不通，点击测试通过后⻜书并不会收到测试消息，这是因为消息

格式体与PrometheusAlert中的⾃定义模版不匹配，我们可以通过查看PrometheusAlert组件的⽇志查看 webhook消息是否发送到了PrometheusAlert组件，⽇志内容如下：

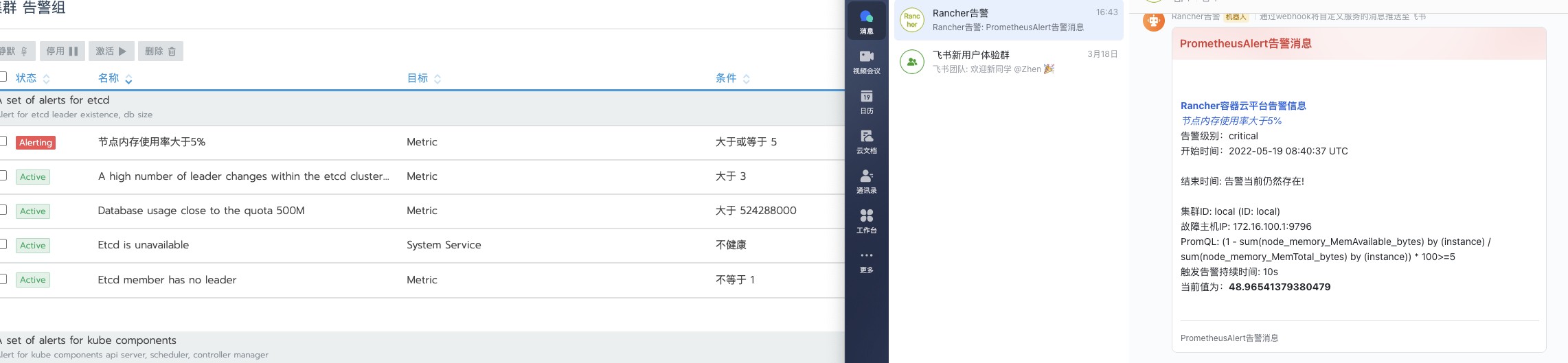
[{"labels":{"test\_msg":"Webhook setting validated"},"annotations":null,"startsAt":"0001-01- 01T00:00:00Z","endsAt":"0001-01-01T00:00:00Z","generatorURL":""}]

SUSE Rancher配置告警通知

上述步骤完成后，我们就可以对告警进⾏通知配置了，在SUSE Rancher UI上进⼊集群/项⽬--⼯具--告警中我们可以对告警/告警组进⾏通知配置，在接收者中配置刚刚添加的Webhook通知



保存后触发告警后就可以发送到⻜书进⾏告警通知了；



故障排查

SUSE Rancher UI测试不通过：检查Rancher Server服务到PrometheusAlert服务的⽹络是否能通讯；

⻜书收不到告警信息：检查PrometheusAlert组件⽇志，查看是否正常发送告警消息到⻜书；

⻜书收到的告警消息有空⽩字段：检查PrometheusAlert中的⾃定义模版，通过测试发送检查告警内容是否错误；

# 总结/感悟

PrometheusAlert全家桶对市⾯上快速迭代的企业沟通⼯具的发送告警⽀持，⽆论通过SUSE Rancher的告警功能或者其他的监控平台都能很好的实现不同客户的⾃定义需求。使⽤⻔槛对于稍微了解Webhook消息和go template基础的⽤户来说都能很快的上⼿，但是想要更好的使⽤PrometheusAlert全家桶可能需要对监控告警体系和go template技能有所要求。

监控/告警体系的建设在本⽂作者看来不是可以⼀蹴⽽就的，⽽是需要⼀定的时间慢慢累计，不断的调整。“狼来了”的告警不应该被视为⼯作上的错误，反⽽这种“狼来了”的告警能够促进监控/告警体系的完善。监控/告警从最开始的后知后觉，慢慢演变为先知先觉，这其中有很⻓的路需要⾛。部分团队可能会觉得运维

⼯程师⽆⾮就是上线部署，重启服务器，删跑路，但正是有了这些“删库跑路”的运维⼯程师，通过正确的预警/监控/告警和深夜⾥处理告警的精神，才避免了⼀次⼜⼀次重⼤的事故。善待运维，完善监控体系，对技术永怀敬畏之⼼；

参考链接

prometheusalert⽂档：https://feiyu563.gitbook.io/prometheusalert/ prometheusalert项⽬：https://github.com/feiyu563/PrometheusAlert/ SUSE Rancher通知：https://docs.rancher.cn/docs/rancher2.5/monitoring-

alerting/configuration/receiver/\_index#webhook

SUSE Rancher告警表达式参考：https://docs.rancher.cn/docs/rancher2.5/monitoring-

alerting/expression/\_index