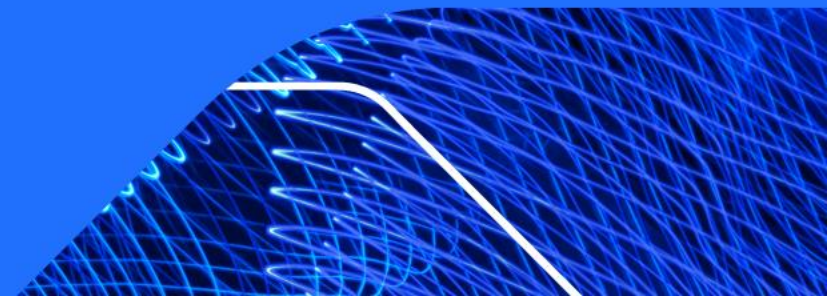
bercut

Prometheus Alert Hints

Александр Голиков
Bercut Ltd

bercut.com info@bercut.com



bercut

аккредитованный российский IT-разработчик и партнер по цифровизации бизнеса

Продукты Bercut являются собственной разработкой, внесены в единый реестр программного обеспечения РФ и соответствуют стандартам отрасли

27 лет

создаем бизнес-ориентированные технологические решения

380+

профессионалов с многолетней экспертизой, знанием рынков, трендов

с 2020 года

Bercut входит в группу Компаний «Ростелеком»

Awards

HIP признан инструментом года для создания цифровых экосистем по версии CNews Awards 2022

О себе

В 2006 красный диплом СПбГЭТУ «ЛЭТИ»

С 2004 по наст. время – ведущий специалист Bercut

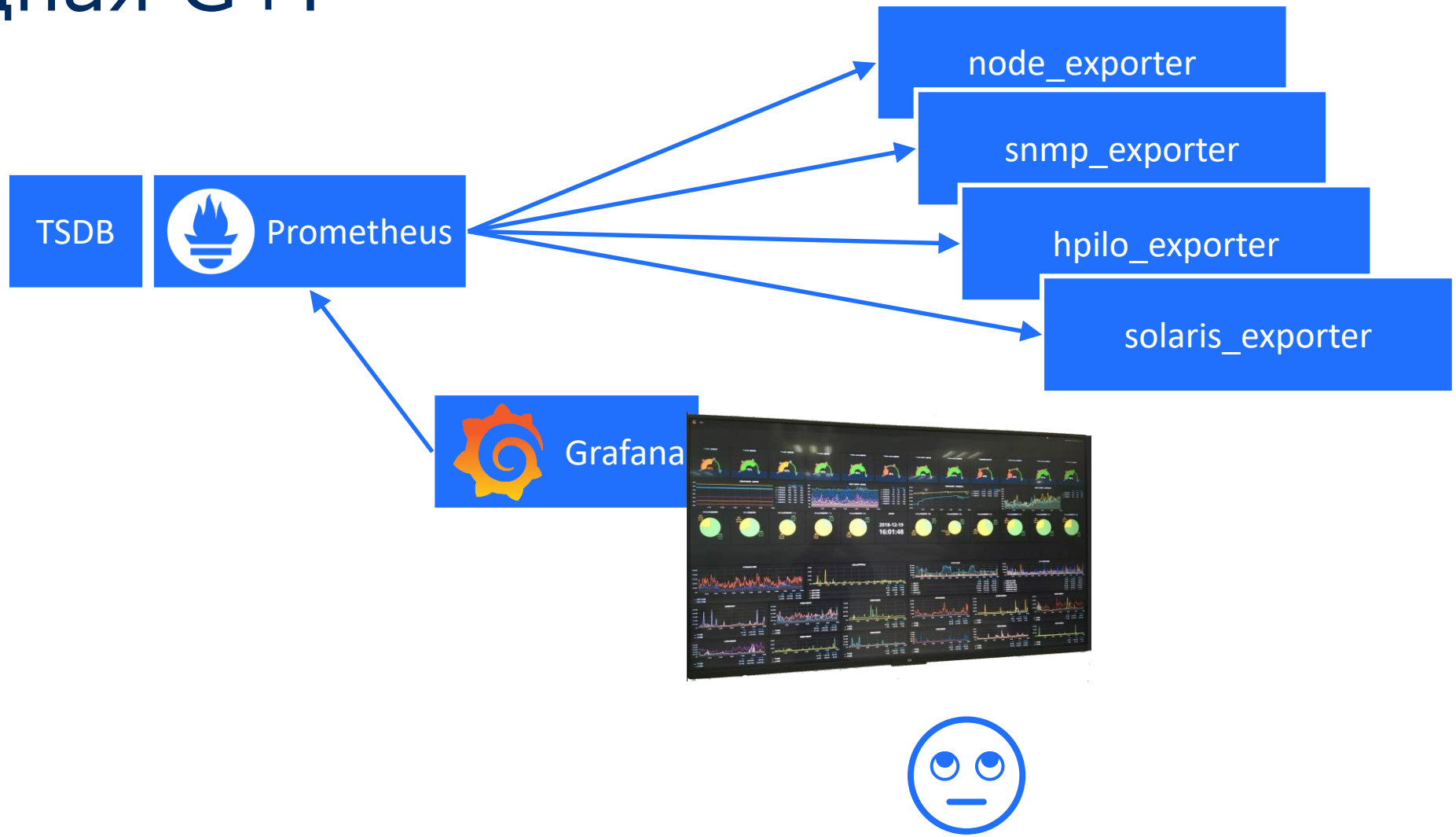
- Виртуализация (KVM, VmWare)
- Storage Area Network, СХД
- Мониторинг (Prometheus, Nagios)
- Unix (SPARC Solaris/Linux)
- Разработка, интеграция продуктов
- Kubernetes
- Kafka

Хобби:
велосипед и прогулки, строительство

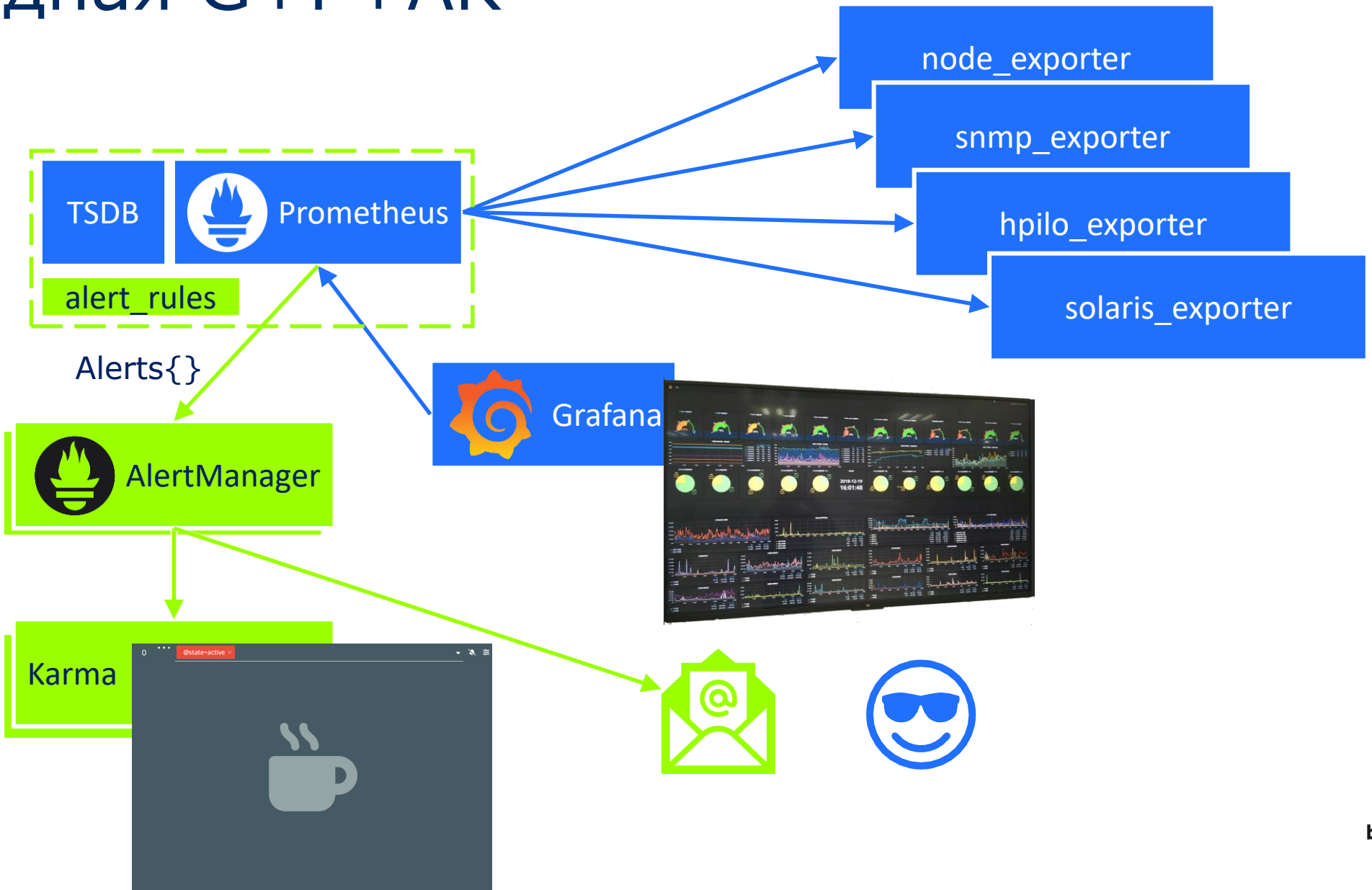
О чём пойдет речь

- Вводная
- Alertmanager в кластере
  - Дашборд алертов Karma
  - Зачем нужен DeadMan
  - Синхронизация настроек
- Написание Alerts
  - Группировка правил, полезные метки
  - Проверка алертов (синтакс и unit-test)
  - Алерты с Go template
  - Сложные пороги срабатывания
  - Иммунитет от алертов (тэг noAlertOn)
- Фиксики (event handlers)

Вводная G+P


node_exporter
snmp_exporter
hpilo_exporter
solaris_exporter
TSDB
Prometheus
Grafana

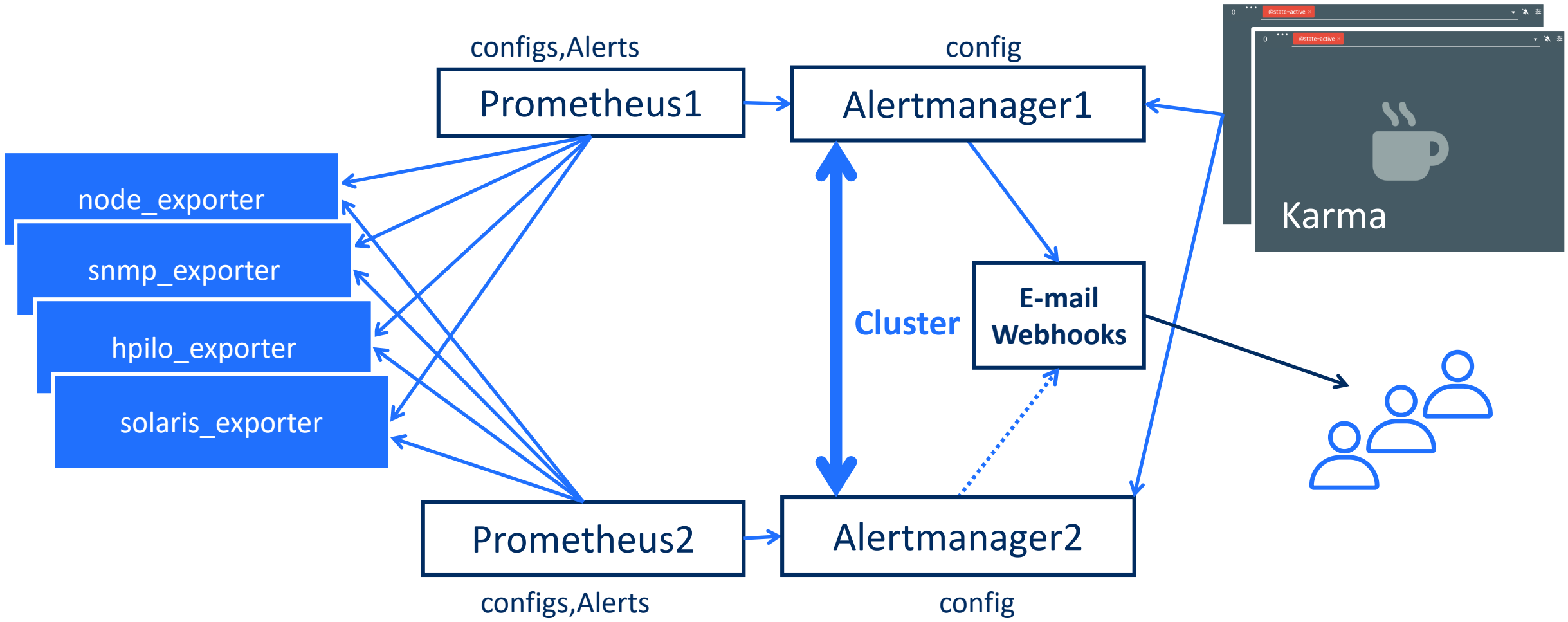
Вводная G+P+AK



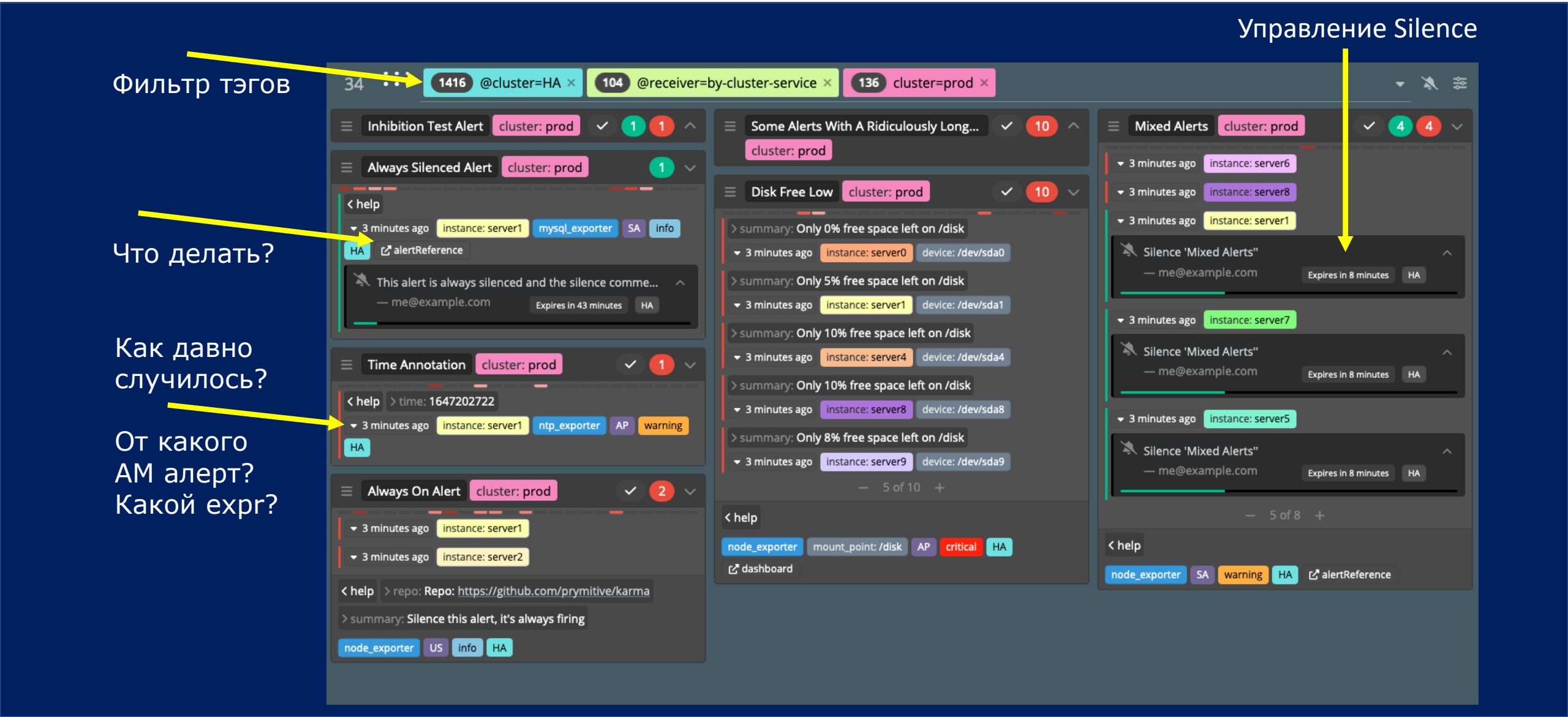
О чём пойдет речь

- Вводная
- Alertmanager в кластере
  - Дашборд алертов Karma
  - Зачем нужен DeadMan
  - Синхронизация настроек
- Написание Alerts
  - Группировка правил, полезные метки
  - Проверка алертов (синтакс и unit-test)
  - Алерты с Go template
  - Сложные пороги срабатывания
  - Иммунитет от алертов (тэг noAlertOn)
- Фиксики (event handlers)

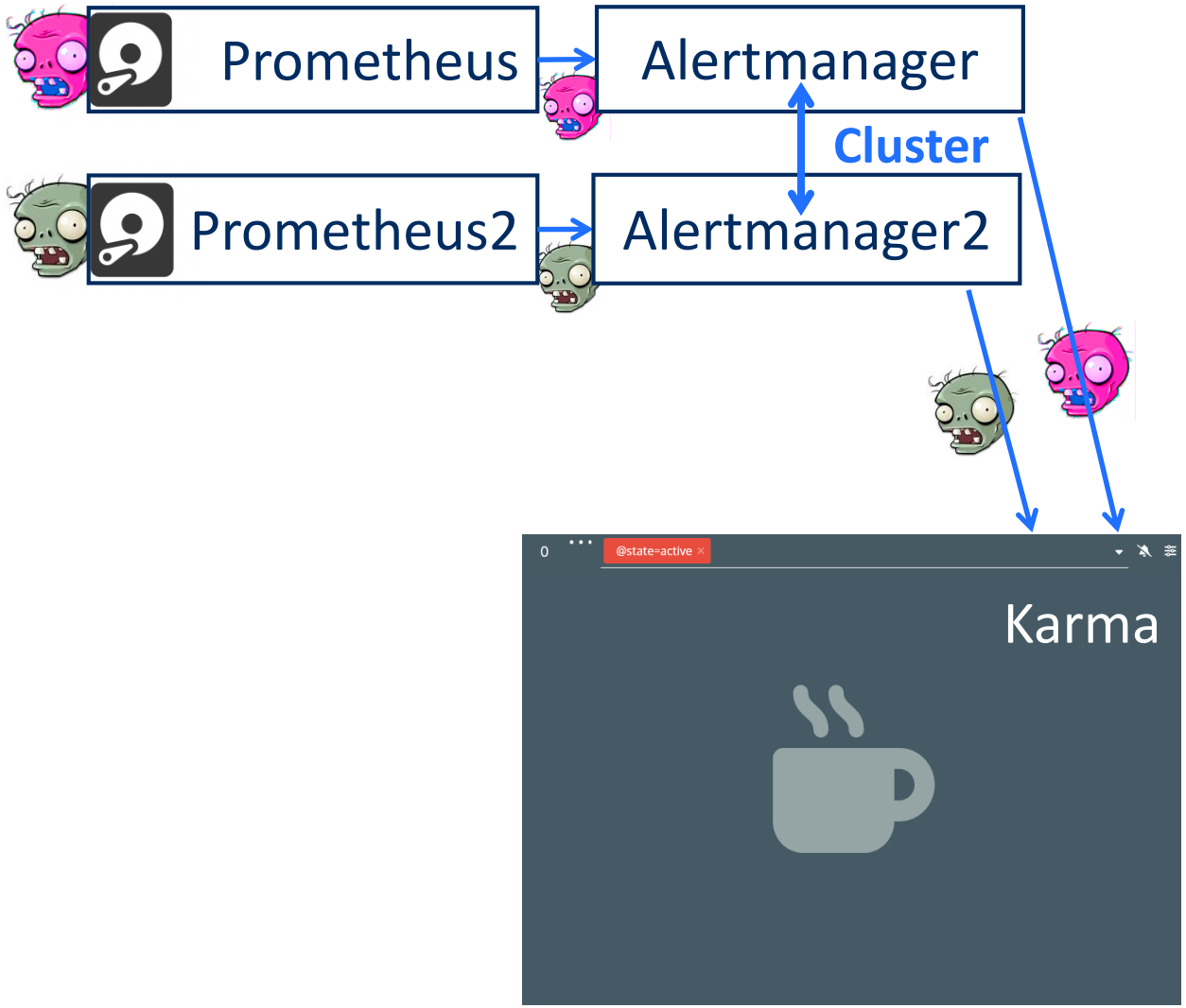
Alertmanager в кластере



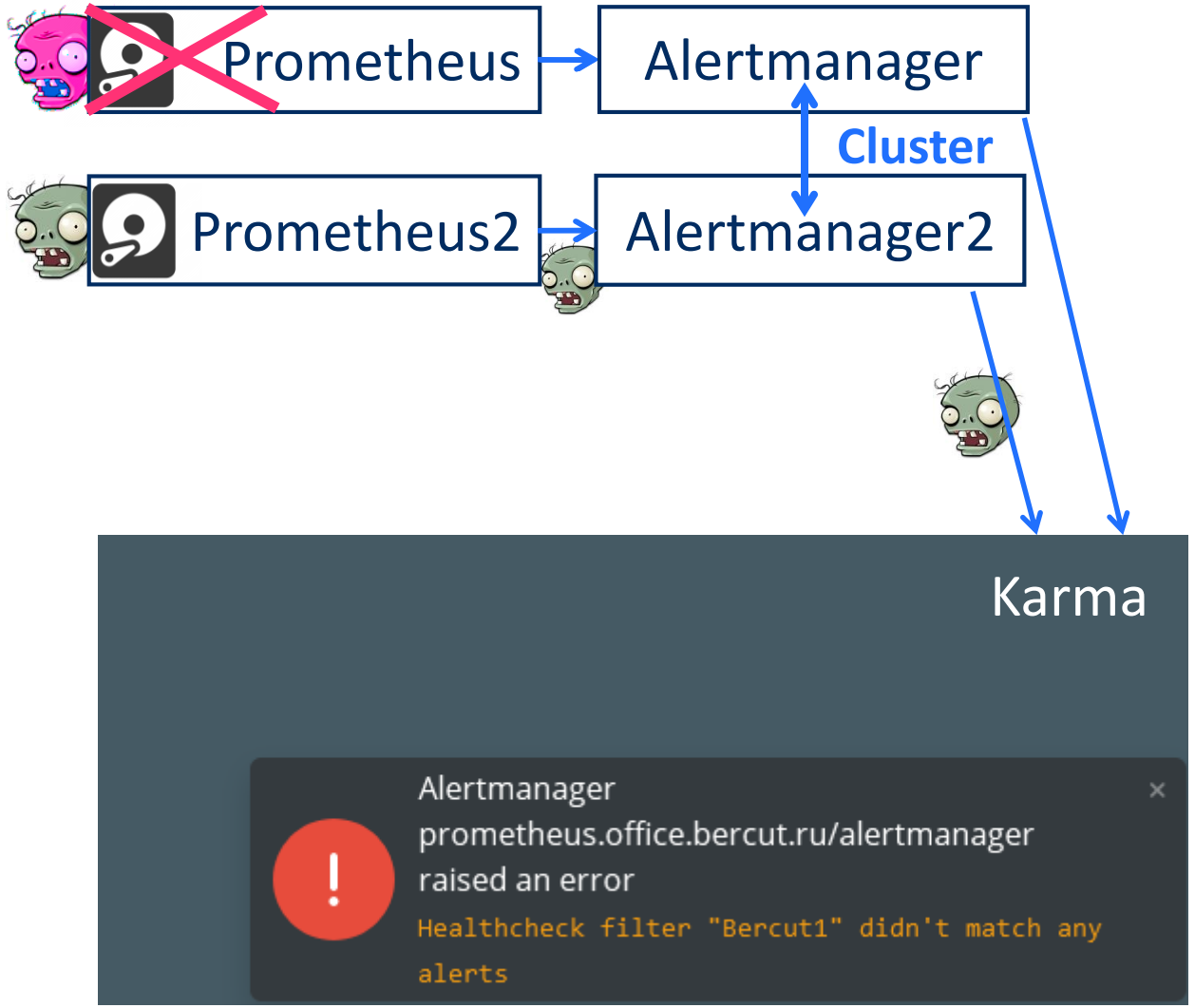
Дашборд алертов Karma



Зачем нужен DeadMan



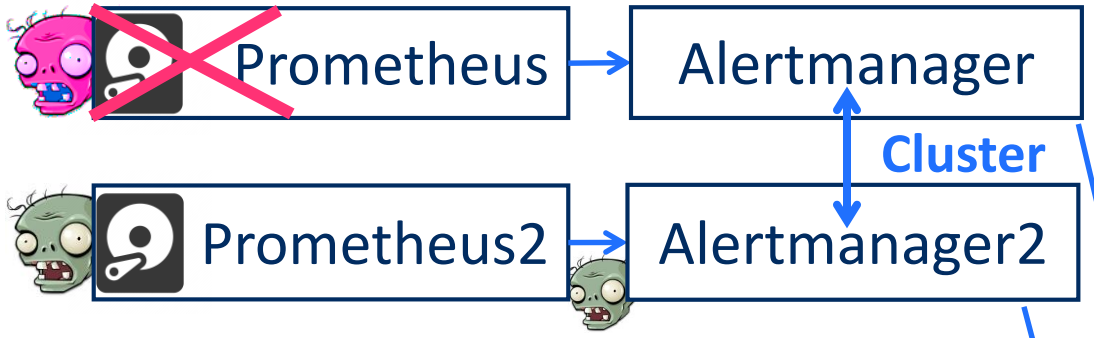
Зачем нужен DeadMan



Зачем нужен DeadMan

prometheus.yml

```
...
rule_files:
   - 'DeadMansSwitch.yml'
...
```

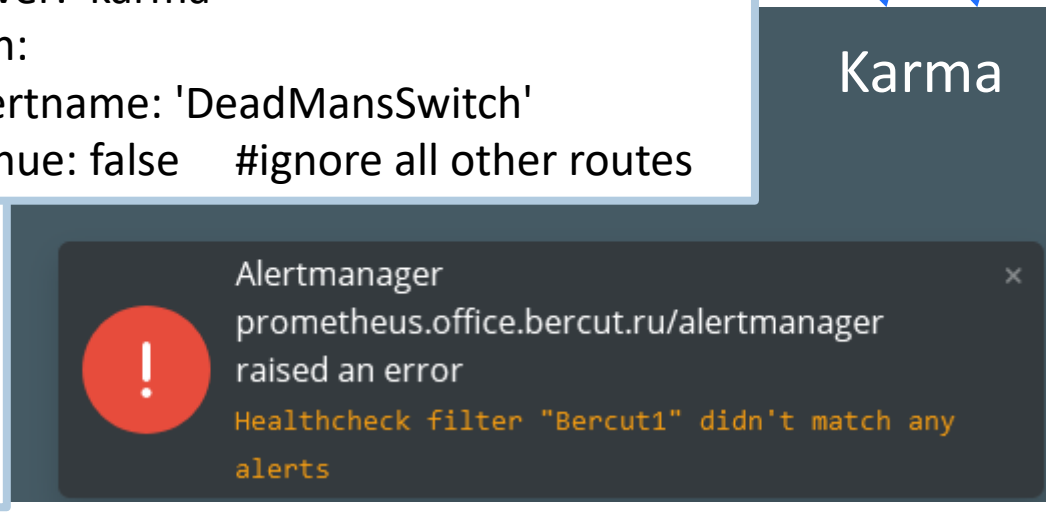


DeadMansSwitch.yml

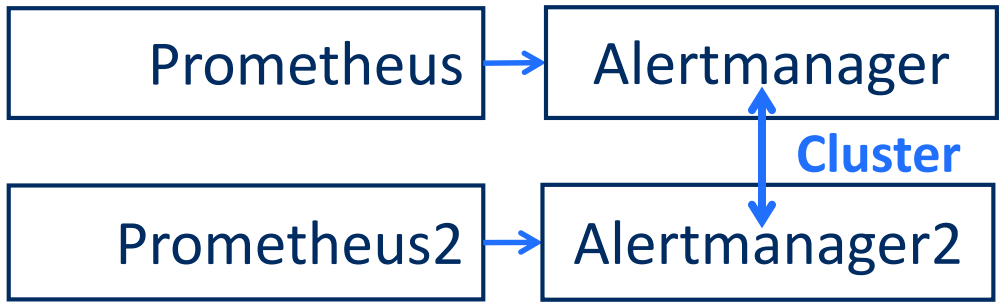
```
groups:
 - name: 'DeadMansSwitch'
   rules:
    - alert: DeadMansSwitch
      expr: vector(1)
      labels:
        prom: 'Bercut1'          # уникальный тэг для каждого узла
      annotations:
        title: 'DeadMansSwitch Alert'
        description: 'This alert should be always ON
                      to check than alert pipeline is working'
```

alertmanager.yml

```
routes:
 - receiver: 'karma'
   match:
      alertname: 'DeadMansSwitch'
   continue: false     #ignore all other routes
```



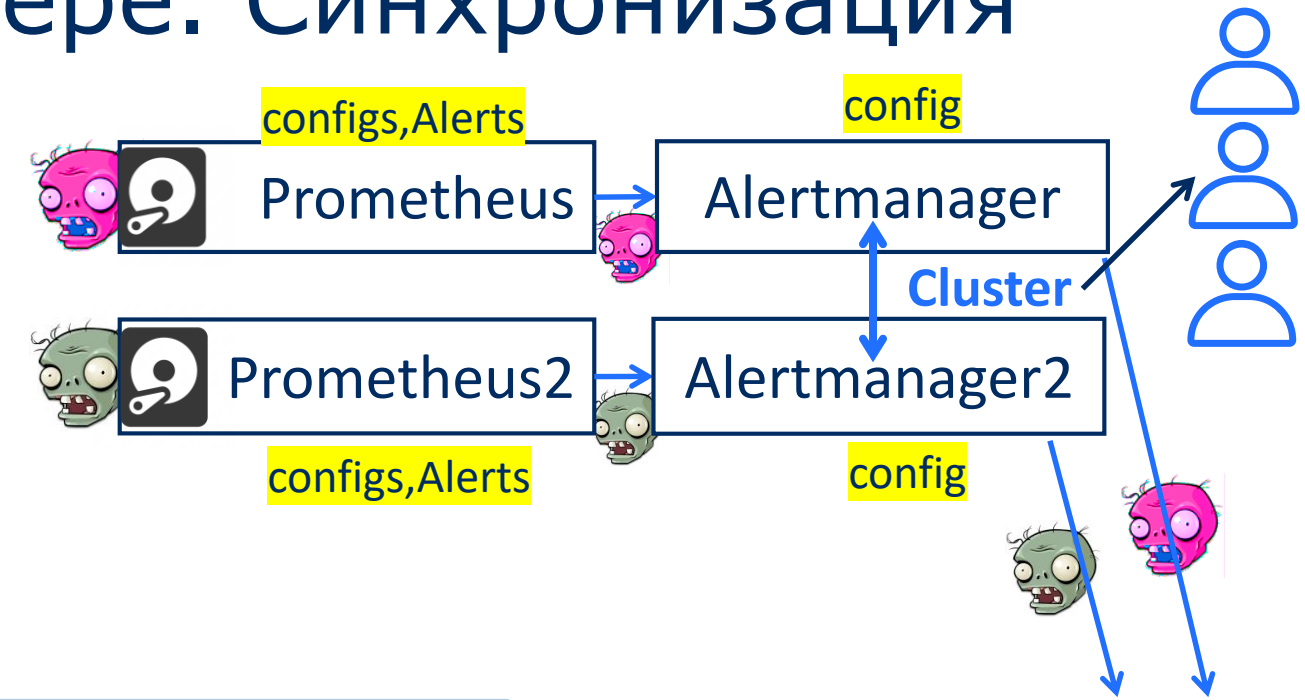
Alertmanager в кластере. Запуск




```
bin/alertmanager \
   --web.listen-address=localhost:9093 \
   --config.file=etc/alertmanager/alertmanager.yml \
   --web.route-prefix=/alertmanager/
   --storage.path=var/alertmanager \
   --cluster.listen-address=0.0.0.0:9094 \
   --cluster.peer=alert2:9094 \
```

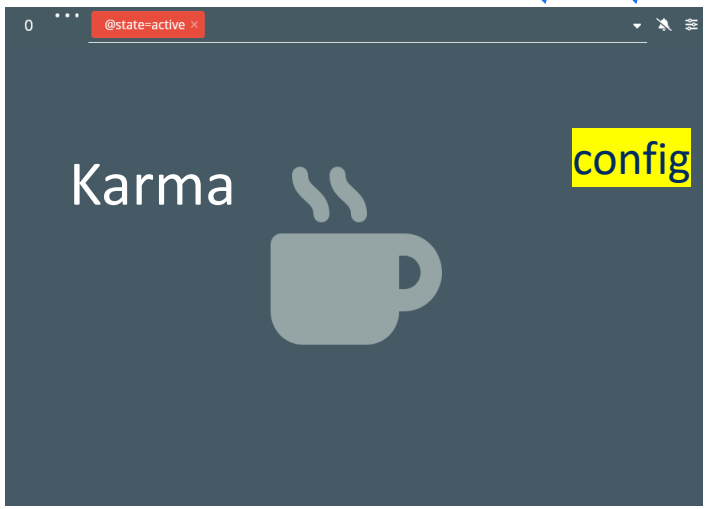
```
bin/alertmanager \
   --web.listen-address=localhost:9093 \
   --config.file=etc/alertmanager/alertmanager.yml \
   --web.route-prefix=/alertmanager/
   --storage.path=var/alertmanager \
   --cluster.listen-address=0.0.0.0:9094 \
   --cluster.peer=alert1:9094 \
```

Alertmanager в кластере. Синхронизация




```
rsync --recursive --relative --links --delete --checksum --group --owner --perms \
        -e "ssh -i ${ssh_key}"  \
        --exclude=${promdir}/etc/DeadMansSwitch.yml  \
        ${file_list} \
        ${promuser}@${remote_host}:/
```

(или git pull для *Infrastructure*-as-*Code)*



О чём пойдет речь

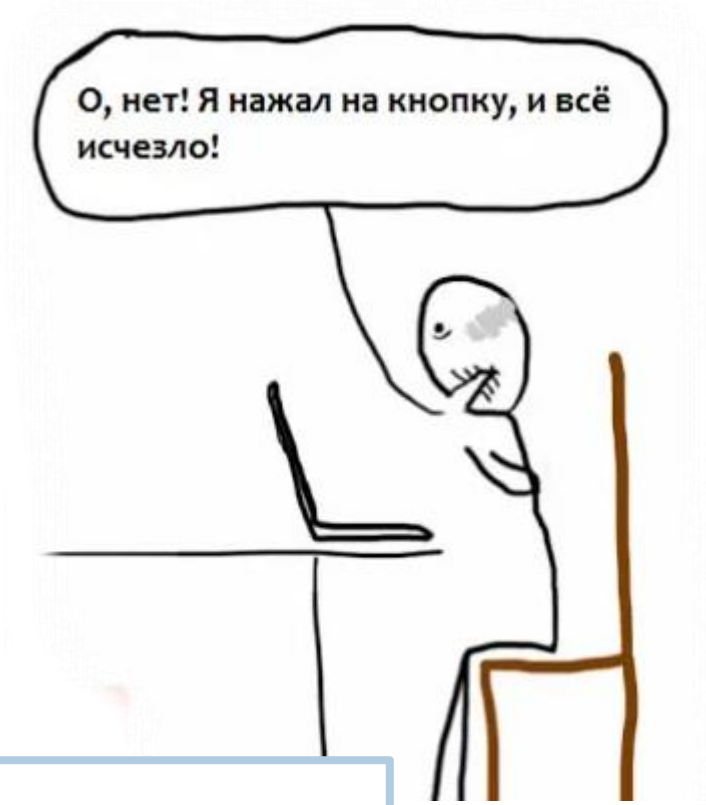
- Вводная
- Alertmanager в кластере
  - Дашборд алертов Karma
  - Зачем нужен DeadMan
  - Синхронизация настроек
- Написание Alerts
  - Группировка правил, полезные метки
  - Проверка алертов (синтакс и unit-test)
  - Алерты с Go template
  - Сложные пороги срабатывания
  - Иммунитет от алертов (тэг noAlertOn)
- Фиксики (event handlers)

Группировка правил алертов

prometheus.yml

```
...
rule_files:
    - 'alerts/alerts.node.yml'
    - 'rules/recording.rules.yml'
    - 'DeadMansSwitch.yml'
# - 'alerts/alerts.apc_snmp.yml'
# - 'alerts/alerts.st2500.yml'
    - 'alerts/alerts.prometheus.yml'
    - 'alerts/alerts.solaris.yml'
    - 'alerts/alerts.blackbox.yml'
    - 'alerts/alerts.ipmi.yml'
    - 'alerts/alerts.hds.g200.yml'
    - 'alerts/alerts.hpe3par.yml'
    - 'alerts/alerts.msl.yml'
    - 'alerts/alerts.hpe_bladechassis.yml'
    - 'alerts/alerts.hpilo.yml'
    - 'alerts/alerts.windows.yml'
    - 'alerts/alerts.brocade.yml'
    - 'alerts/alerts.vmware.yml'
    - 'alerts/alerts.msa.yml'
    - 'alerts/alerts.backups.yml'
    - 'alerts/alerts.build.yml'
    - 'alerts/alerts.postgres.yml'
    - 'alerts/alerts.e9000.yml'
    - 'alerts/alerts.hus_ams.yml'
    - 'alerts/alerts.MIB.yml'
    - 'alerts/alerts.raid.yml'
    - 'alerts/alerts.speed-test.yml'
    - 'alerts/alerts.kafka.yml'
    - 'alerts/alerts.IPscript.yml'
    - 'alerts/alerts.pve.yml'
    - 'alerts/alerts.serverview.yml'
    - 'alerts/alerts.oradb_connect.yml'
    - 'alerts/alerts.billing.yml'
    - 'alerts/alerts.huaweisw.yml'
...
```

Полезные метки алертов




```
Node Exporter is down
Node exporter 10.10.10.10 does not return any metrics!
```

```
# ssh 10.10.10.10
ssh: connect to host 10.10.10.10 port 22: No route to host
```

Полезные метки алертов

Node Exporter is down

Node exporter does not return any metrics

Check host availability, check process is running.

severity:	critical
alertReference:	https://www.youtube.com/watch?v=dQw4w9WgXcQ
owner:	dba
os:	linux
hostname:	mydb102
sc:	10.10.11.10
BladeChassis:	plat198c7000

Полезные метки алертов

alerts/alerts.node.yml

```
- alert: 'Node_exporter_service'
    expr: up{job="node_exporter"} == 0
    for: 10m
    labels:
      severity: 'critical'
    annotations:
      title: "Node Exporter is down"
      description: 'Node exporter does not return any metrics!
                    Check host availability, check process is running.'
      alertReference: 'https://www.youtube.com/watch?v=dQw4w9WgXcQ'
```

prometheus.yml

```
- job_name: 'node_exporter'
    file_sd_configs:
      - files:
        - 'inventory/*.yml'
    relabel_configs:
      ...
      - source_labels: [__address__]
        regex: (.*)
        replacement: ${1}:9100
        target_label: __param_target
```

inventory/10.10.10.10.yml

```
- targets:
  - 10.10.10.10
  labels:
    jobs: "node_exporter,blackbox-ssh,hpilo,mpath,hperaid"
    owner: "dba"
    os: "linux"
    hostname: "mydb102"
    sc: 10.10.11.10
    vsp: plat198c7000
```

Проверки алертов. Синтакс.

Проверка синтаксиса:

```
bin/promtool check config etc/prometheus.yml
echo -e "Check result code is $?"
```

Примеры найденых ошибок:

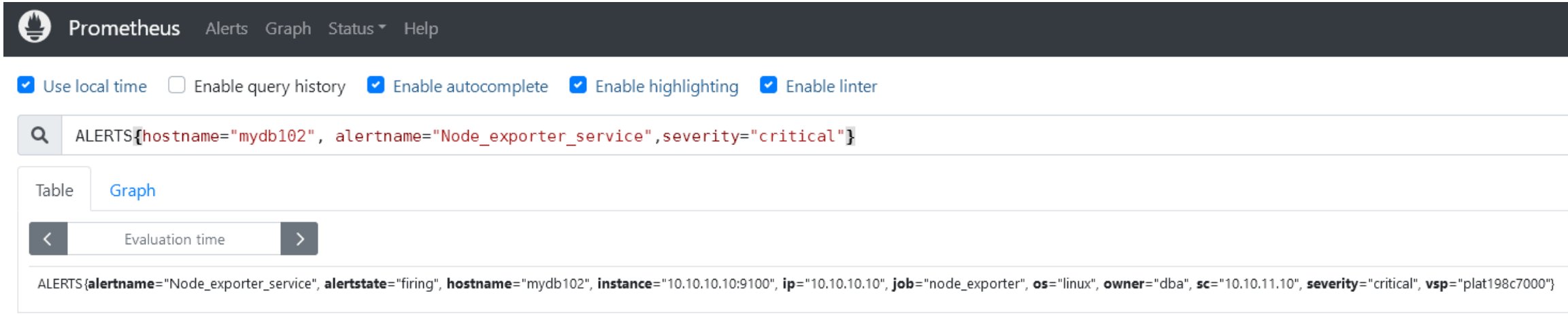
```
Checking alerts/alerts.node.yml
  FAILED:
    alerts/alerts.node.yml: group "Node exporter alerts", rule 1, "Node_exporter_service": annotation
"description": template: __alert_Node_exporter_service:1: function "blababala" not defined
```

или

```
Checking /opt/prometheus/etc/alerts/alerts.node.yml
  FAILED:
    alerts/alerts.node.yml: yaml: line 11: did not find expected key
```

Проверки алертов. Вживую.

1)



2) Выполнение запроса к метрике ALERTS в CLI:

**bin/promtool query instant "http://localhost:9090/prometheus" **
"ALERTS{hostname='mydb102',alertname='Node_exporter_service',severity='critical'}"

ALERTS{alertname="Node_exporter_service", alertstate="firing", hostname="mydb102", instance="10.10.10.10:9100", ip="10.10.10.10", job="node_exporter", os="linux", owner="dba", sc="10.10.11.10", severity="critical", vsp="plat198c7000"} => 1 @[1674550246.995]

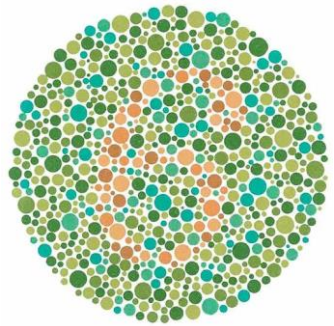
3) Выполнение запроса к Prometheus через API

curl 'http://localhost:9090/prometheus/api/v1/alerts' | jq

Проверки алертов. Unit test

bin/promtool test rules unit-test.yml

Unit Testing: unit-test.yml
 SUCCESS



Тут 6 =)

unit-test.yml

```
rule_files:
    - alerts/alerts.node.yml
evaluation_interval: 1m
tests:
    - interval: 1m
      input_series:
          - series: 'up{hostname="mydb102",instance="10.10.10.10:9100",ip="10.10.10.10",
                     job="node_exporter", os="linux",owner="dba",sc="10.10.11.10",severity="critical",
                     vsp="plat198c7000"}'
            values: '0 0 0 0 0 0 0 0 0 0 0 0 0 0 0'
      alert_rule_test:
          - eval_time: 10m
            alertname: 'Node_exporter_service'
            exp_alerts:
                - exp_labels:
                      severity: 'critical'
                      instance: "10.10.10.10:9100"
                      job: "node_exporter"
                      ip: "10.10.10.10"
                      hostname: "mydb102"
                      os: "linux"
                      owner: "dba"
                      sc: "10.10.11.10"
                      vsp: "plat198c7000"
                  exp_annotations:
                      title: "Node Exporter is down"
                      description: "Node exporter does not return any metrics!
                                    Check host availability, check process is running."
                      alertReference: "https://www.youtube.com/watch?v=dQw4w9WgXcQ"
```

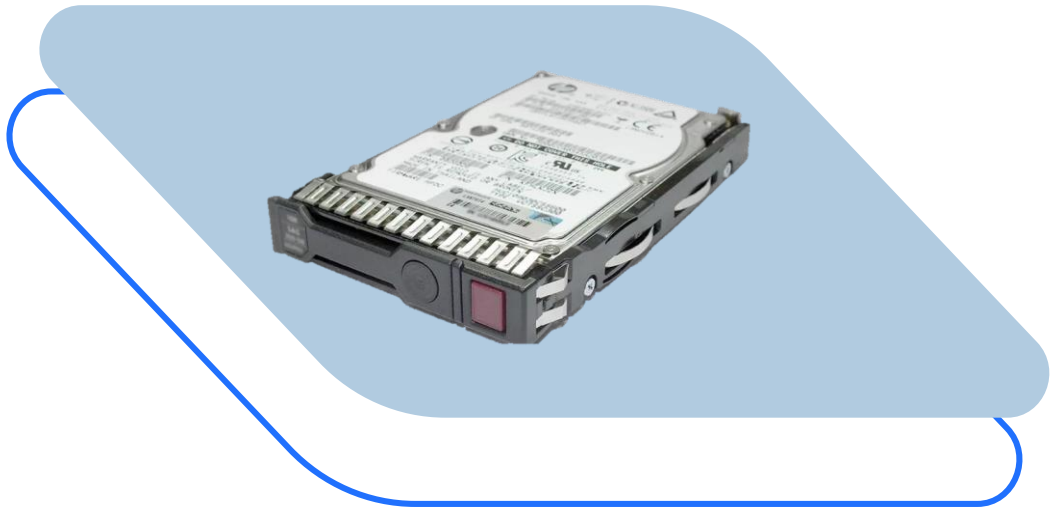
Алерты с Go template, if, eq, query

```
hpe_raid_message{hostname="mydb102", ip="10.10.10.10", job="hperaid", owner="dba", sc="10.10.11.10", vsp="plat198c7000",
    message="RAID WARNING - Component Failure: Array A logicaldrive 1 (1.64 TB, RAID 1+0, OK) Array B logicaldrive 2 (3.27 TB, RAID 5,
OK) physicaldrive 1I:3:3 (port 1I:box 3:bay 3, SAS HDD, 900 GB, Predictive Failure)"}  1
hpe_raid_status{hostname=" mydb102", ip="10.10.10.10", job="hperaid", owner="dba", sc="10.10.11.10", vsp="plat198c7000"}      1
```

Сообщение

Статус

```
0 - ok
1 - warning
2 - critical
3 - unknown
```



hperaid on 10.10.10.10 has problems
hperaid check on host 10.10.10.10 mydb102 has returned Warning status (1).
RAID WARNING - Component Failure: Array A logicaldrive 1 (1.64 TB, RAID 1+0, OK) Array B logicaldrive 2 (3.27 TB, RAID 5, OK) physicaldrive 1I:3:3 (port 1I:box 3:bay 3, SAS HDD, 900 GB, Predictive Failure)

Алерты с Go template, if, eq, query

```
hpe_raid_message{hostname="mydb102", ip="10.10.10.10", job="hperaid", owner="dba", sc="10.10.11.10", vsp="plat198c7000",
    message="RAID WARNING - Component Failure: Array A logicaldrive 1 (1.64 TB, RAID 1+0, OK) Array B logicaldrive 2 (3.27 TB, RAID 5,
OK) physicaldrive 1I:3:3 (port 1I:box 3:bay 3, SAS HDD, 900 GB, Predictive Failure)"}  1
hpe_raid_status{hostname=" mydb102", ip="10.10.10.10", job="hperaid", owner="dba", sc="10.10.11.10", vsp="plat198c7000"}        1
```

```
- alert: 'hperaid_result'
  expr: hpe_raid_status{} != 0
  for: 10m
  labels:
    severity: warning
  annotations:
    title: 'hperaid on {{ .Labels.ip }} has problems'
    description: "hperaid check on host {{ .Labels.ip }} {{ .Labels.hostname }} has returned
                  {{      if eq (.Value | humanize) \"0\"  }} OK
                  {{ else if eq (.Value | humanize) \"1\"  }} Warning
                  {{ else if eq (.Value | humanize) \"2\"  }} Critical
                  {{ else if eq (.Value | humanize) \"3\"  }} Unknown
                  {{ end }} status
                  ({{ .Value | printf \"%.0f\" }}).
                  {{ with printf \"hpe_raid_message{ip='%s',job='%s'}\"
                                  .Labels.ip .Labels.job | query }}
                  {{ . | first | label \"message\" }}
                  {{end}}"
```

```
type sample struct {
    Labels map[string]string
    Value float64
}
```

→ или $labels.

→ или $value

hperaid on 10.10.10.10 has problems

hperaid check on host 10.10.10.10 mydb102 has returned Warning status (1).

RAID WARNING - Component Failure: Array A logicaldrive 1 (1.64 TB, RAID 1+0, OK) Array B logicaldrive 2 (3.27 TB, RAID 5, OK) physicaldrive 1I:3:3 (port 1I:box 3:bay 3, SAS HDD, 900 GB, Predictive Failure)

Алерты с Go template, if, eq, query:UnitTest

unit-test.yml

```
input_series:
 - series: 'hpe_raid_message{hostname="mydb102", ip="10.10.10.10", job="hperaid", owner="dba", sc="10.10.11.10", vsp="plat198c7000",message="RAID WARNING -
Component Failure: Array A logicaldrive 1 (1.64 TB, RAID 1+0, OK) Array B logicaldrive 2 (3.27 TB, RAID 5, OK) physicaldrive 1I:3:3 (port 1I:box 3:bay 3, SAS HDD,
900 GB, Predictive Failure)"}'
   values: '1 1 1 1 1 1 1 1 1 1 1 1 1 1 1'
 - series: 'hpe_raid_status{hostname=" mydb102", ip="10.10.10.10", job="hperaid", owner="dba", sc="10.10.11.10", vsp="plat198c7000"}'
   values: '1 1 1 1 1 1 1 1 1 1 1 1 1 1 1'
alert_rule_test:
 - eval_time: 11m
   alertname: hperaid_result'
```

alerts/alerts.node.testrule.yml: group "Testing alerts", rule 3, "hperaid_result": annotation "description": template: __alert_hperaid_result:1: unexpected "}" in operand

```
bin/promtool test rules unit-test.yml
Unit Testing:  unit-test.yml
  FAILED:
    alertname: hperaid_result, time: 11m,
        exp:[
            0:
              Labels:{alertname="hperaid_result"}
              Annotations:{}
            ],
        got:[
            0:
              Labels:{alertname="hperaid_result", hostname=" mydb102", ip="10.10.10.10", job="hperaid", owne
severity="warning", vsp="plat198c7000"}
              Annotations:{description="hperaid check on host 10.1
has returned  Warning  status (1).  RAID WARNING - Component
logicaldrive 1 (1.64 TB, RAID 1+0, OK) Array B logicaldrive
5, OK) physicaldrive 1I:3:3 (port 1I:box 3:bay 3, SAS HDD, 9
Failure) ", title="hperaid on 10.10.10.10 has problems"}
```

hperaid on 10.10.10.10 has problems
hperaid check on host 10.10.10.10 mydb102 has returned Warning status (1).
RAID WARNING - Component Failure: Array A logicaldrive 1 (1.64 TB, RAID 1+0, OK) Array B logicaldrive 2 (3.27 TB, RAID 5, OK) physicaldrive 1I:3:3 (port 1I:box 3:bay 3, SAS HDD, 900 GB, Predictive Failure)

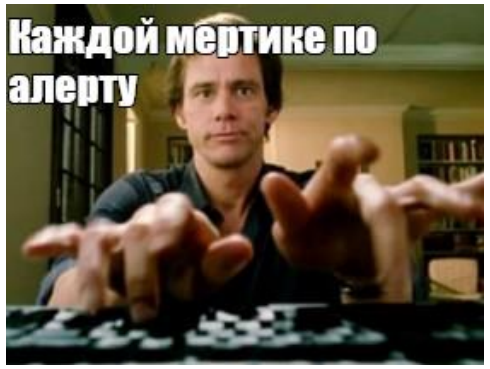
Алерты с Go template, dynamic labels

```
hpilo_battery_status     0
hpilo_bios_hardware_status 1
hpilo_fan_status 0
hpilo_memory_status 2
hpilo_power_supply_status 0
hpilo_processor_status 0
hpilo_running_status 0
hpilo_storage_controller_health_status 0
hpilo_storage_enclosure_health_status 0
hpilo_storage_ld_health_status 0
hpilo_storage_pd_health_status 0
```

```
severity:
0 - ok
1 - warning
2 - critical
3 - warning
```

Статус = severity

много метрик -> одно правило алерта



Алерты с Go template, dynamic labels

```
hpilo_battery_status     0
hpilo_bios_hardware_status 1
hpilo_fan_status 0
hpilo_memory_status 2
hpilo_power_supply_status 0
hpilo_processor_status 0
hpilo_running_status 0
hpilo_storage_controller_health_status 0
hpilo_storage_enclosure_health_status 0
hpilo_storage_ld_health_status 0
hpilo_storage_pd_health_status 0
```

```
severity:
0 - ok
1 - warning
2 - critical
3 - warning
```

```
- alert: 'HWstatus'
  expr: '{job="hpilo", __name__=~"hpilo_.*status"} > 0'
  for: 0s
  labels:
    severity: "{{ if or ( eq ($value) 1.0 ) ( eq ($value) 3.0 }}warning
               {{ else }}critical{{ end }}"
    metric: '{{ .Labels.__name__ }}'
  annotations:
      ...
```

одно правило
два алерта

```
0:
        Labels:{alertname="HWstatus", metric="hpilo_bios_hardware_status",
severity="warning"}
1:
        Labels:{alertname="HWstatus", metric="hpilo_memory_status",
severity="critical"}
```

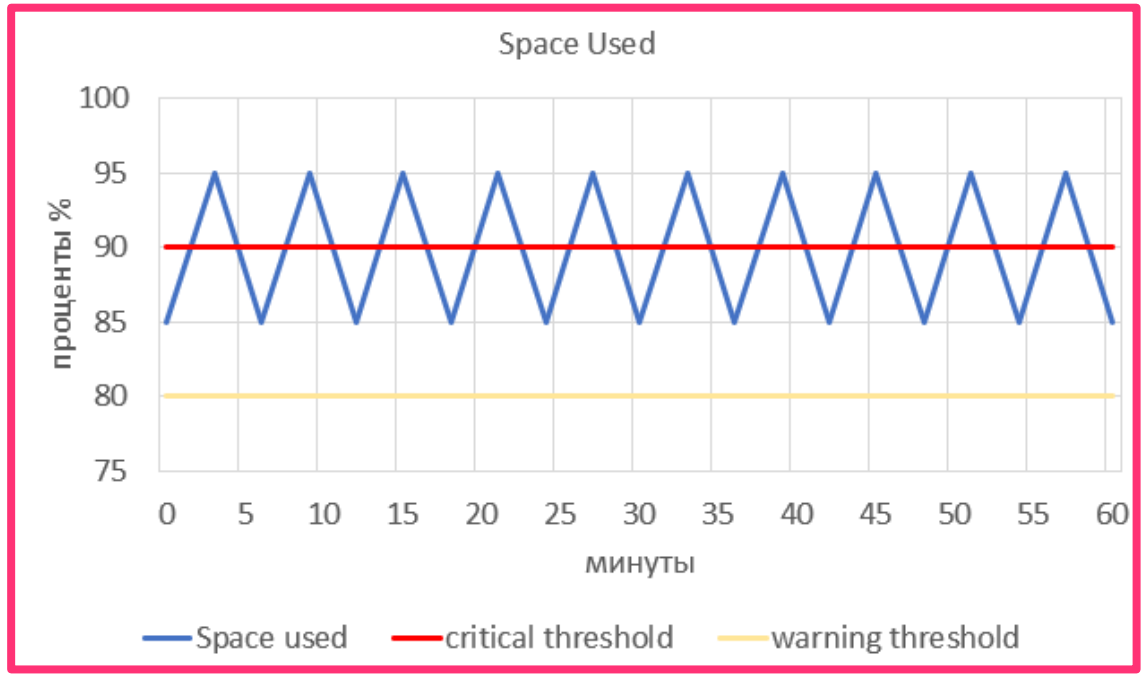
Алерты с Go template, ~~dynamic labels~~

```
hpilo_battery_status     0
hpilo_bios_hardware_status 1
hpilo_fan_status 0
hpilo_memory_status 2
hpilo_power_supply_status 0
hpilo_processor_status 0
hpilo_running_status 0
hpilo_storage_controller_health_status 0
hpilo_storage_enclosure_health_status 0
hpilo_storage_ld_health_status 0
hpilo_storage_pd_health_status 0
```

```
severity:
0 - ok
1 - warning
2 - critical
3 - warning
```

```
- alert: 'HWstatus'
  expr: 'space_used_on_disk_percent > 80'
  for: 10m
  labels:
    severity: "{{ if lt ($value) 90.0 ) }}warning
               {{ else }}critical{{ end }}"
  annotations:
      ...
```

?

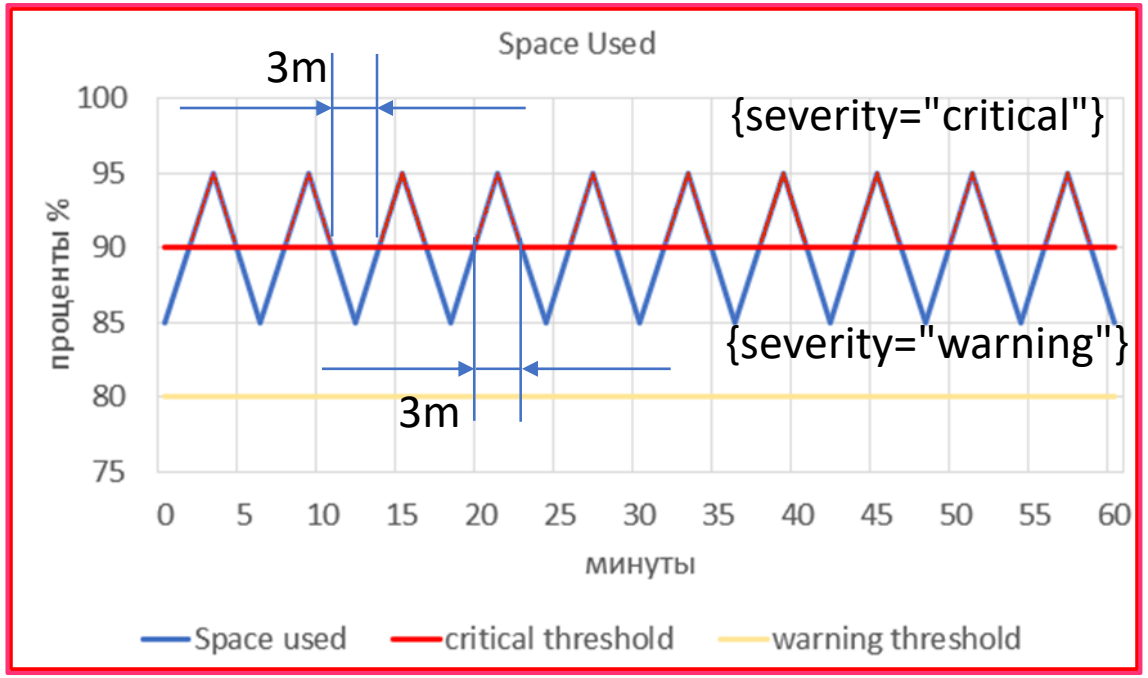


bercut

Алерты с Go template, ~~dynamic labels~~

Проблема есть, а алерта НЕТ!
Нет даже warning

```
- alert: 'HWstatus'
  expr: 'space_used_on_disk_percent > 80'
  for: 10m
  labels:
    severity: "{{ if lt ($value) 90.0 ) }}warning
               {{ else }}critical{{ end }}"
  annotations:
      ...
```



Алерты без dynamic labels

alerts/alerts.node.yml

```
  - alert: 'DiskSpace'
    expr: space_used_on_disk_percent > 80
    for: 10m
    labels:
      severity: "warning"
        ...
 - alert: 'DiskSpace'
    expr: space_used_on_disk_percent > 90
    for: 10m
    labels:
      severity: "critical"
        ...
```

alertmanager.yml

```
inhibit_rules:
  - source_match:
      severity: 'critical'
    target_match:
      severity: 'warning'
    equal: ['alertname', 'instance' ]
```

Алерты с Go template, добавленные тэги

```
Mib_LBR_Status{instance="10.10.10.31", job="MIB"}                  1
Mib_SMSC_Status{instance="10.10.10.32", job="MIB"}                 1
Mib_USSDC_Status{instance="10.10.10.33", job="MIB"}                0
Mib_MNP_WII_SCPwii_Status{instance="10.10.10.34", job="MIB"}       1
```

```
expr: '{job="MIB",__name__=~"Mib_.*_Status"} !=1'
```


```
Some application is not running on host 10.10.10.33
```

Алерты с Go template, добавленные тэги

```
Mib_LBR_Status{instance="10.10.10.31", job="MIB"}                  1
Mib_SMSC_Status{instance="10.10.10.32", job="MIB"}                 1
Mib_USSDC_Status{instance="10.10.10.33", job="MIB"}                0
Mib_MNP_WII_SCPwii_Status{instance="10.10.10.34", job="MIB"}       1
```

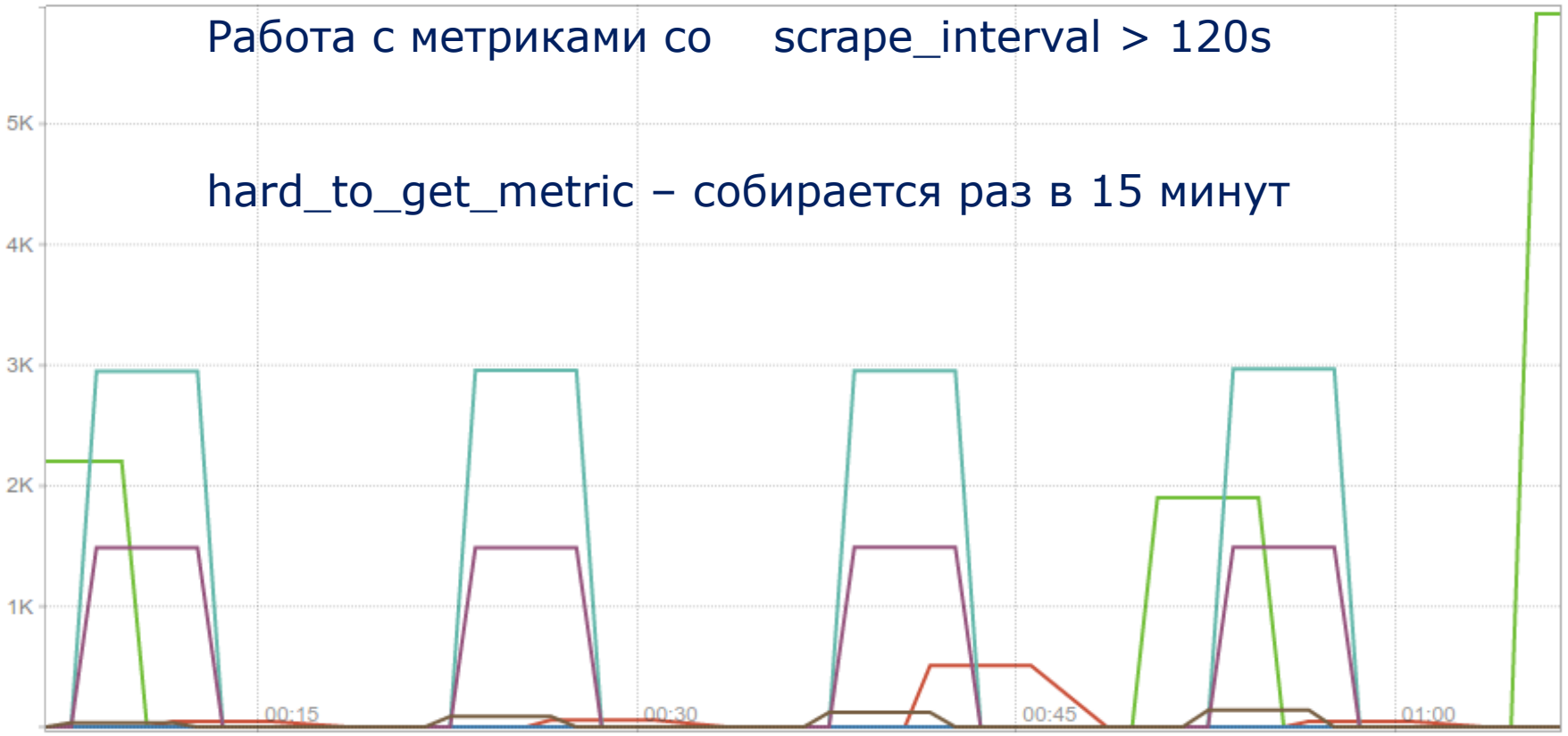
```
- alert: 'Application is not running'
   #expr: '{job="MIB",__name__=~"Mib_.*_Status"} !=1'
   expr: 'label_replace(
               {job="MIB",__name__=~"Mib_.*_Status"},
               "Application",
                "$1", "__name__",
                "Mib_(.*)_Status"
               )
               != 1'
   for: 0s
   labels:
     severity: 'warning'
   annotations:
     title: '{{ .Labels.Application }} is not running'
     description: 'Metric Mib_{{ .Labels.Application }}_Status
                   on host {{ .Labels.instance }} shows that
                    {{ .Labels.Application }} is not running'
```

USSDC is not running
Metric Mib_USSDC_Status on host 10.10.10.33
shows that USSDC is not runing

```
Labels:{
alertname="Application is not running",
instance="10.10.10.33",
Application="USSDC",
severity="warning"}
```

bercut

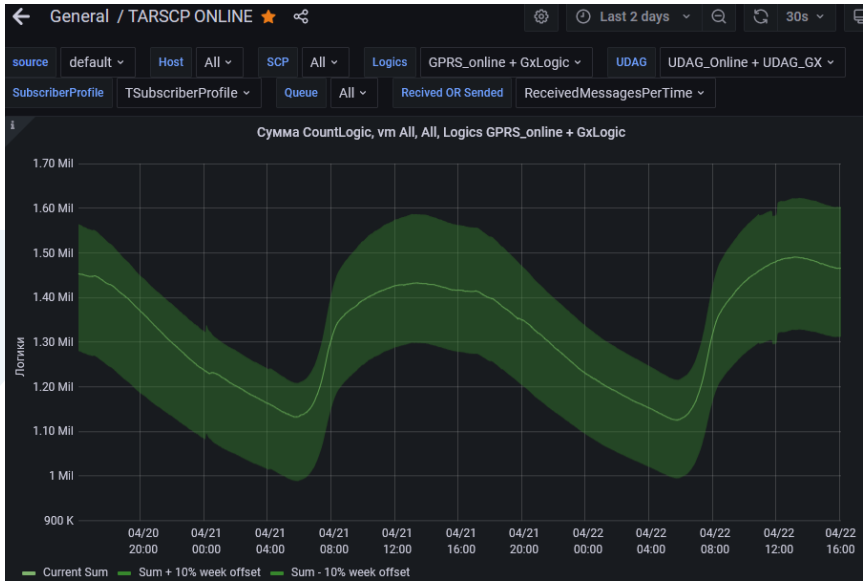
Сложные пороги срабатывания, *_over_time



expr: max_over_time(hard_to_get_metric[900s])

Сложные пороги срабатывания, offset

```
expr: 'abs(
       100 * (
              Mib_SCP_ONLINE_CountLogic_counter
              -
              (Mib_SCP_ONLINE_CountLogic_counter{} offset 1w)
             )
            /
           (Mib_SCP_ONLINE_CountLogic_counter{} offset 1w)
       )
       > 10'
```



Сравнение со значением метрики неделю назад

Иммунитет от алертов (тэг noAlertOn)

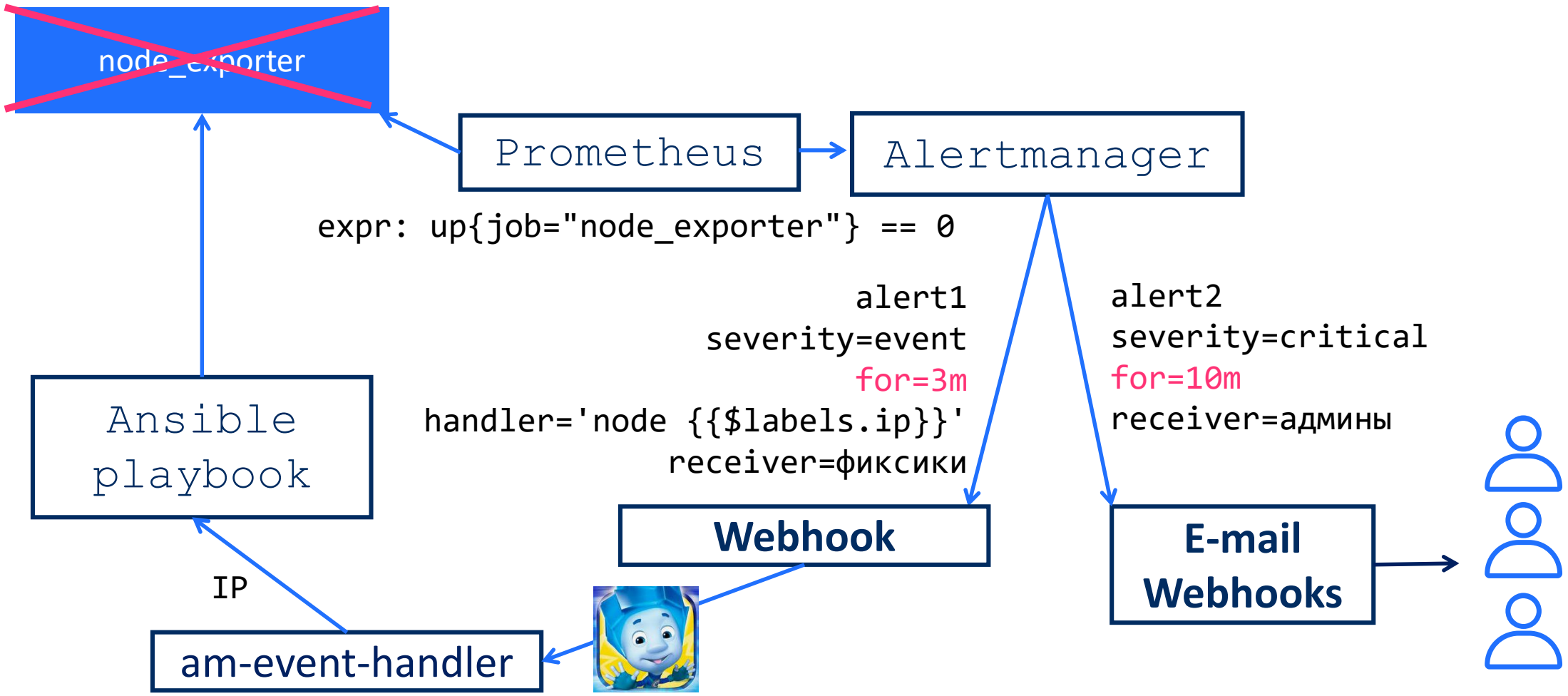
```
- targets:
  - 10.10.10.10
  labels:
    jobs: "node_exporter,blackbox-ssh,hpilo,mpath,hperaid"
    owner: "dba"
    hostname: "mydb102"
    sc: 10.10.11.10
    vsp: plat198c7000
    noAlertOn: "bond,space"
```

```
 - alert: "Bond degraded"
    expr: (node_bonding_active{ noAlarmOn!~"(.*,|^)bond(,.*|$)" }
                                                    - node_bonding_slaves) != 0
    for: 1m
    labels:
      severity: 'warning'
    annotations:
      title: "Bonding status"
      description: 'Bond {{ $labels.master }} is degraded.'
```

О чём пойдет речь

- Вводная
- Alertmanager в кластере
  - Дашборд алертов Karma
  - Зачем нужен DeadMan
  - Синхронизация настроек
- Написание Alerts
  - Группировка правил, полезные метки
  - Проверка алертов (синтакс и unit-test)
  - Алерты с Go template
  - Сложные пороги срабатывания
  - Иммунитет от алертов (тэг noAlertOn)
- Фиксики (event handlers)

Фиксики (event handlers)



Ссылки

- Наборы готовых алертов awesome-prometheus-alerts
- O unit testing в prometheus
- Онлайн демо дашборд Karma
- Дашборд Karma
- Event Handler (Фиксики)
- Go Temlate syntax & Go Template Online validation
- Ссылки на затронутые проблемы Q1 Q2 Q3
- Solaris exporter
- HP iLO exporter
- Инструмент по экпорту/импорту дашбордов в Grafana Grafana-Import-Export

Вопросы?

Hosts: 850	Targets: 3.5 K	Alert Rules: 365 active, 20 disabled
Samples per second: 11 K	Scrape internal 10-240 sec, avg 60 sec	Number of Series: 575 K
cores 4 ram 16G	TSDB Prom(2 weeks) 23G	TSDB VM(7 months) 75G

bercut.com

Нельзя так просто взять и прекратить меряться