

TRUE custom monitoring

The journey to success

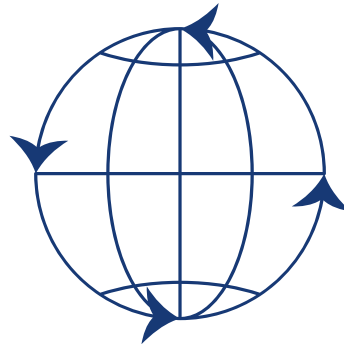


Whoami?

Brian van Baekel



- Zabbix consultant
- Zabbix trainer
- Network engineer



Opensource ICT Solutions

Whoami?

Nathan Liefiting



- Network engineer
- Zabbix management/enthusiast

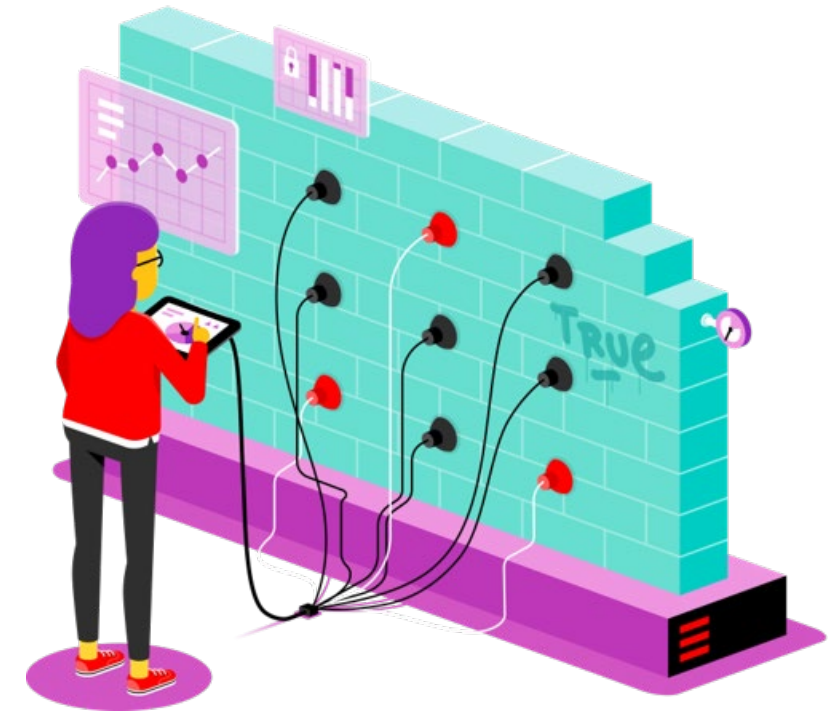
TRUE

Current situation

- Monitoring




- Servers




- Network


Old situation



OverviewDevicesPortsHealthWirelessRoutingAlerts






0



Global Search

Dashboards:Default




Device-summary-horiz









	Total	Up	Down	Ignored	Disabled
Devices	236	214	9	10	3
Ports	25223	17789	2542	875	2818

Availability-map

Total hosts up: 214 warn: 0 down: 9



Alerts

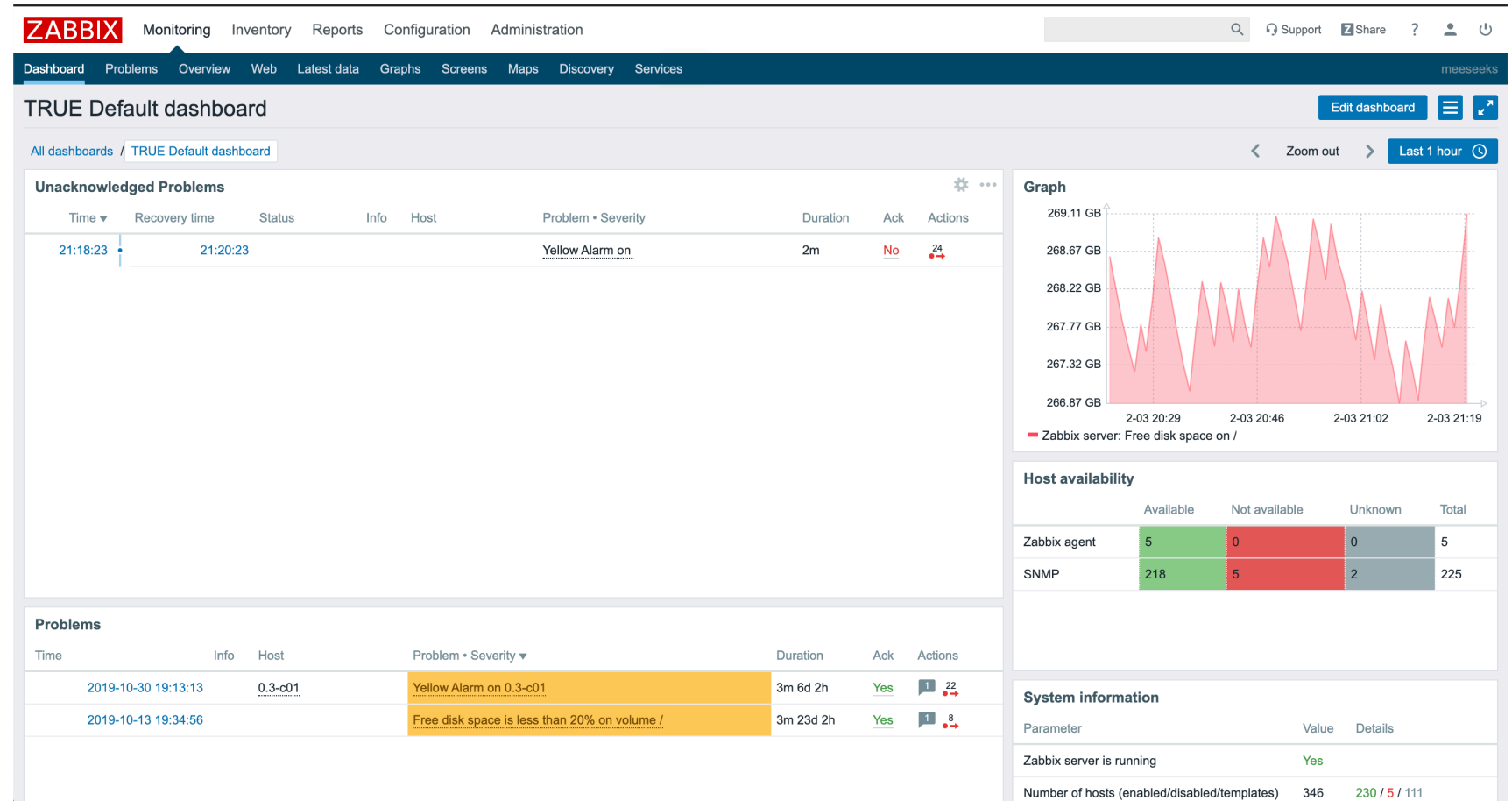
2019-11-28 08:16:01	Devices up/down less important	pre_transpoc_01		
2019-10-28 15:05:01	Internal eBGP session down	gateway01		
2019-10-15 08:16:01	Memory over limit	gateway01		
2019-10-15 08:16:01	Storage over limit	gateway01		

Current situation

- Dashboard

Dashboards

- ☐ Name ▲
- ☐ TRUE Core Routers
- ☐ TRUE Default dashboard
- ☐ TRUE Maps
- ☐ TRUE Zabbix server health



Old situation

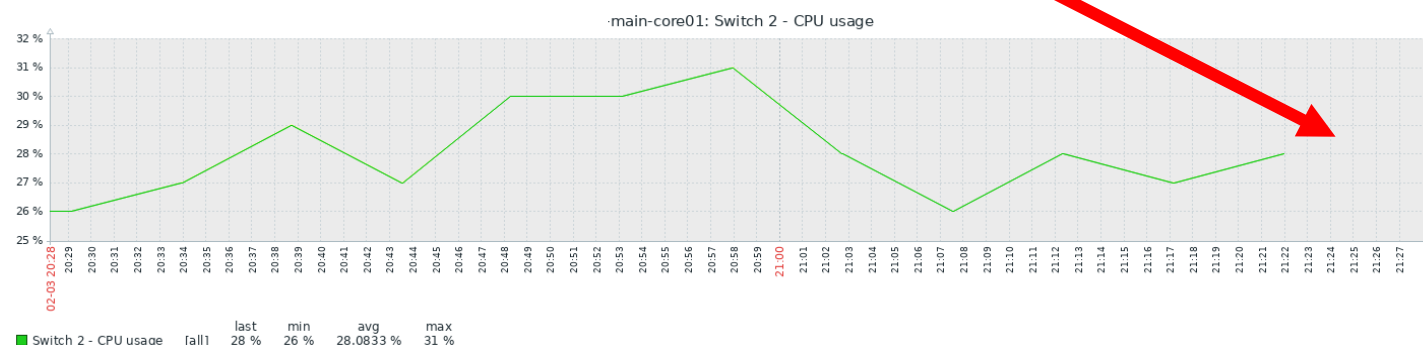
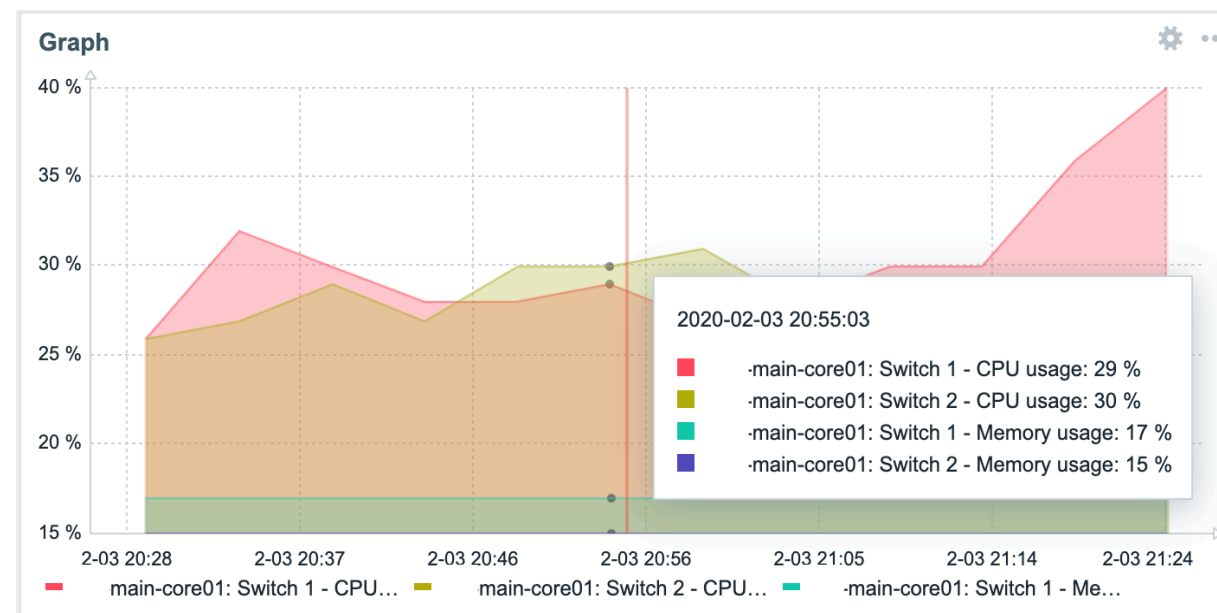
- LibreNMS Graphing



Current situation














- Zabbix Graphing

Bug!
(ZBX-1977)



Old situation

- LibreNMS Alerting

<div><div></div><div>Overview Devices Ports Health Wireless Routing Alerts</div><div><div>0</div><div></div><div><input type="text" value="Global Search"/></div></div></div>							
#	Name	Rule	Severity	Status	Extra	Enabled	Action
<div><div>+ Create new alert rule</div> - OR - <div>+ Create rule from collection</div></div>							50
#1	Devices up/down	<code>macros.device_down = 1</code>	critical	!	Max: -1 Delay: 1 Interval: 300	<div>ON</div>	<div> </div>
#2	Device rebooted	<code>devices.uptime < 300 AND macros.device = 1</code>	warning	✓	Max: 1 Delay: 5 Interval: 300	<div>ON</div>	<div> </div>
#3	iBGP Session down	<code>bgpPeers.bgpPeerState != "established" AND macros.device_up = 1 AND bgpPeers.bgpPeerRemoteAs = 15703</code>	critical	✓	Max: -1 Delay: 5 Interval: 3600	<div>ON</div>	<div> </div>
#4	BGP Session established	<code>bgpPeers.bgpPeerFsmEstablishedTime < 300 AND bgpPeers.bgpPeerState = "established"</code>	ok		Max: 1 Delay: 0 Interval: 300	<div>OFF</div>	<div> </div>
#5	Port down now	<code>macros.port_now_down = 1 AND devices.hostname NOT REGEXP ".*drac.*" AND devices.hostname NOT REGEXP ".*mgmt.*" AND devices.device_id != 72 AND devices.device_id != 46 AND devices.device_id != 92 AND devices.device_id != 248 AND ports.port_id != 71402</code>	warning	!	Max: -1 Delay: 5 Interval: 10800	<div>ON</div>	<div> </div>

Current situation



Nathan Liefing
larcorba

Edit profile

The Netherlands

Overview **Repositories 7** Projects 0 Packages 0 Stars 1 Followers 0 Following 1

Find a repository... Type: All Language: All **New**

opsgenie-integration ★ Star
Forked from opsgenie/opsgenie-integration
Python 40 Apache License 2.0 Updated 3 days ago

Larcorba-Zabbix-templates-Juniper-QFX5200-SNMPv3 ★ Star
★ 1 Updated on 17 Nov 2019

Larcorba-Zabbix-templates-Juniper-QFX5110-SNMPv3 ★ Star
★ 1 Updated on 17 Nov 2019

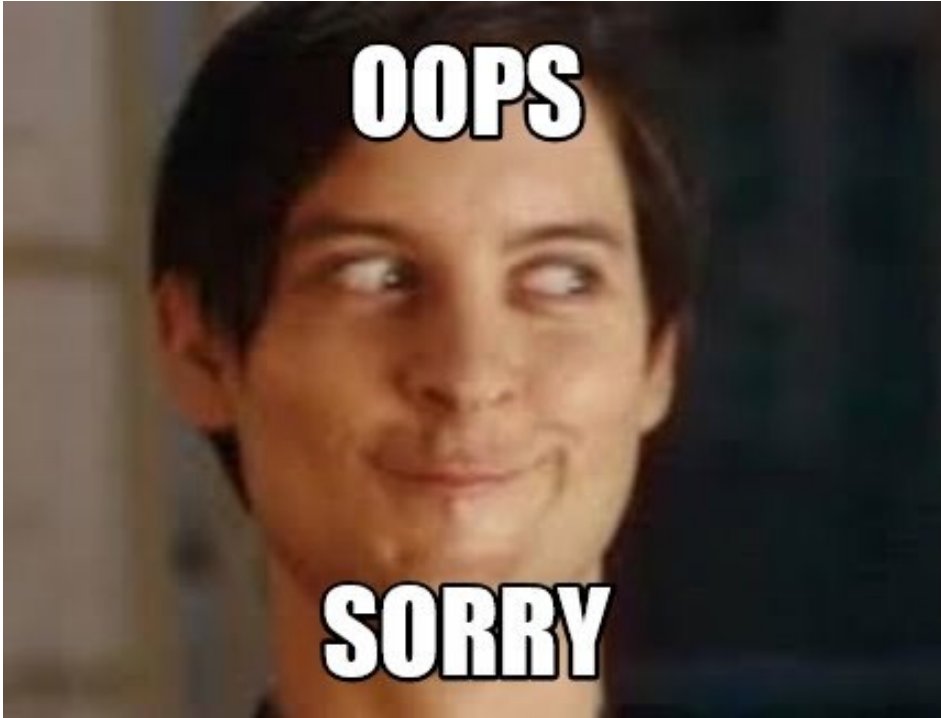
Larcorba-Zabbix-templates-Fortigate-General-SNMPv3 ★ Star
Updated on 17 Nov 2019

Larcorba-Zabbix-templates-Juniper-EX-SNMPv3 ★ Star
★ 1 Updated on 17 Nov 2019

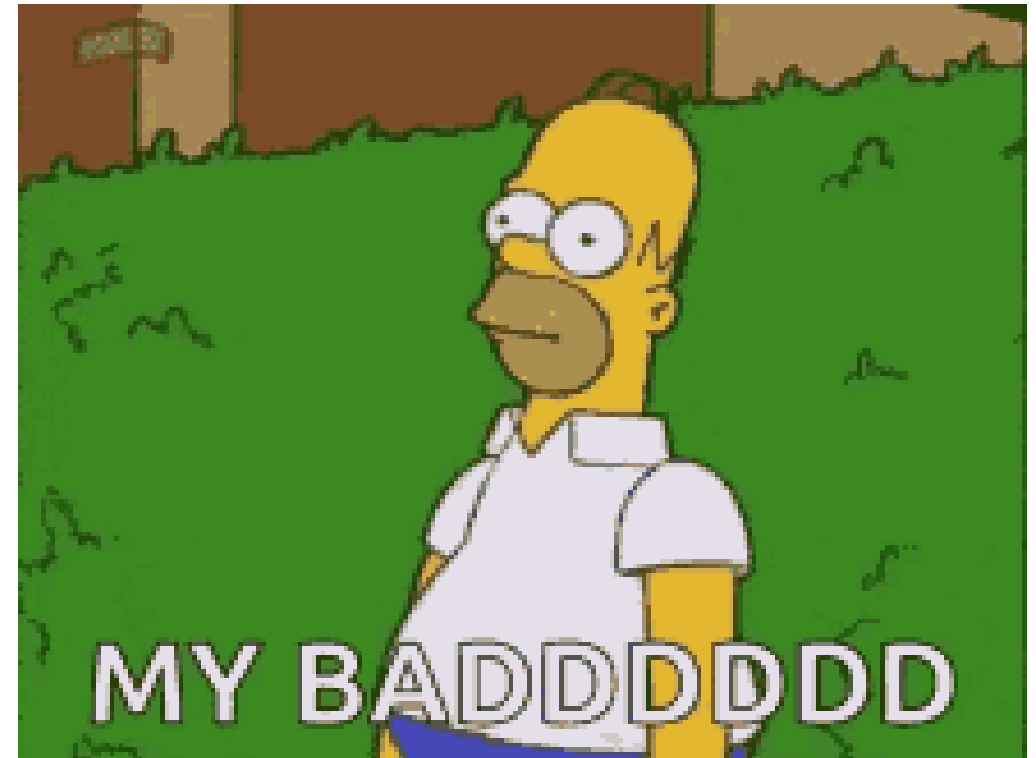
Larcorba-Zabbix-templates-Juniper-MX-SNMPv3 ★ Star
★ 1 Updated on 17 Nov 2019

- Zabbix Alerting

Old situation



- Automation



```
import requests
import json

url = "https://meeseeks.true.nl/api_jsonrpc.php"
```

```
def get_api_token(url):

    payload = {
        "jsonrpc": "2.0",
        "method": "user.login",
        "params": {"user": "python-api", "password":
        "id": 1,
        "auth": None
    }

    resp = requests.post(url=url, json=payload )
    out = resp.json()

    return out['result']
```

```
def get_hosts(api_token, url):

    payload = {
        "jsonrpc": "2.0",
        "method": "host.get",
        "params": {
            "output": [
                "hostid",
                "host"
            ],
            "selectInterfaces": [
                "interfaceid",
                "ip",
                "main"
            ]
        },
        "id": 2,
        "auth": api_token
    }

    resp = requests.post(url=url, json=payload )
    out = resp.json()

    return out['result']
```

Current situation

- Automation



- Autofill /etc/hosts file on our jump host 'Unity' using the Zabbix API

Current situation

- Alerting
- Telegram
- Opsgenie



Meeseeks Bot 17:41

PROBLEM ▼

PROBLEM: ·hybrid-02 1 - CPU usage above 80% (Warning)
Host: ·hybrid-02
I'm Mr. Meeseeks look at me!



Meeseeks Bot 17:46

OK ▼

OK: € ·ybrid-02 1 - CPU usage above 80% (Warning)
Host: € ·ybrid-02
Ooooh, okay!

Current situation

- OpsGenie why? How?

Zabbix + OpsGenie

All Categories

Notifications & Alerting

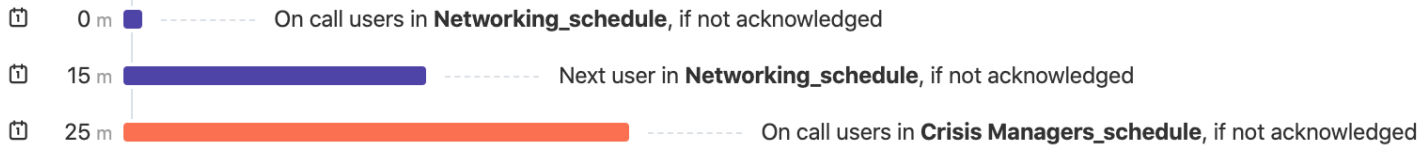
Official Templates

Current situation

- OpsGenie why? How?

Escalation policies

Networking_escalation



20:49 93%

Alerts

en Critical Unack'd Closed Unseen All

P3 #63 x1 **CLOSED**

[Zabbix] Unavailable by ICMP ping

4d, Nathan Liefing

P3 #62 x1 **CLOSED**

[Zabbix] Unavailable by ICMP ping

4d, Nathan Liefing

P3 #61 x1 **CLOSED**

[Zabbix] Unavailable by ICMP ping

4d, Nathan Liefing

Current situation

- OpsGenie integration caveats

 [ZABBIX FEATURE REQUESTS / ZBXNEXT-5586](#)
Opsgenie webhook integration

ZABBIX Zabbix (Zabbix)

+ Create Alert

↕ Create Alert 

↕ Create Alert 

+ Close Alert

↕ Close Alert 

+ Acknowledge Alert

↕ Acknowledge Alert 

Current situation

- OpsGenie solution

ZABBIX Zabbix (Zabbix)

Acknowledge Alert

↑ Acknowledge Alert ⚙

Settings >

Filter

Match all conditions below

-- Equals Value

Date

Event Id

Host Name

IP Address

Item Key

Item Value

Recipients

Recovery

Event Status

Responders

Current situation

ZABBIX Zabbix (Zabbix)

- OpsGenie solution

```
func parseFlags()map[string]string{
    apiKey := flag.String("apiKey", "", "apiKey")

    triggerName := flag.String("triggerName", "", "TRIGGER.NAME")
    triggerId := flag.String("triggerId", "", "TRIGGER.ID")
    triggerStatus := flag.String("triggerStatus", "", "TRIGGER.STATUSEVENT.ACK.STATUS")
    triggerSeverity := flag.String("triggerSeverity", "", "TRIGGER.SEVERITY")
    triggerDescription := flag.String("triggerDescription", "", "TRIGGER.DESRIPTION")
    triggerUrl := flag.String("triggerUrl", "", "TRIGGER.URL")
    triggerValue := flag.String("triggerValue", "", "TRIGGER.VALUE")
    triggerHostGroupName := flag.String("triggerHostGroupName", "", "TRIGGER.HOSTGROUP.NAME")
    hostName := flag.String("hostName", "", "HOSTNAME")
    ipAddress := flag.String("ipAddress", "", "IPADDRESS")
    date := flag.String("date", "", "DATE")
    time := flag.String("time", "", "TIME")
    itemKey := flag.String("itemKey", "", "ITEM.KEY")
    itemValue := flag.String("itemValue", "", "ITEM.VALUE")
    eventId := flag.String("eventId", "", "EVENT.ID")
    recoveryEventStatus := flag.String("recoveryEventStatus", "", "EVENT.RECOVERY.STATUS")
    tags := flag.String("tags", "", "tags")
    responders := flag.String("responders", "", "responders")
    logPath := flag.String("logPath", "", "LOGPATH")
}
```

Settings

Filter

Match all conditions below

Trigger St... ▾

-- ▾

Equals ▾

PROBLEMYes

[+ Add new condition](#)

Current situation

- OpsGenie solution

Jan 31, 2020 3:06 PM

⚡ alertAction • System

Alert acknowledged via
Zabbix[Zabbix-Acknowledge Alert] with
incomingDataId[5ef52b09-31e3-47a0-baf0-5a56
8ed6dc2e]

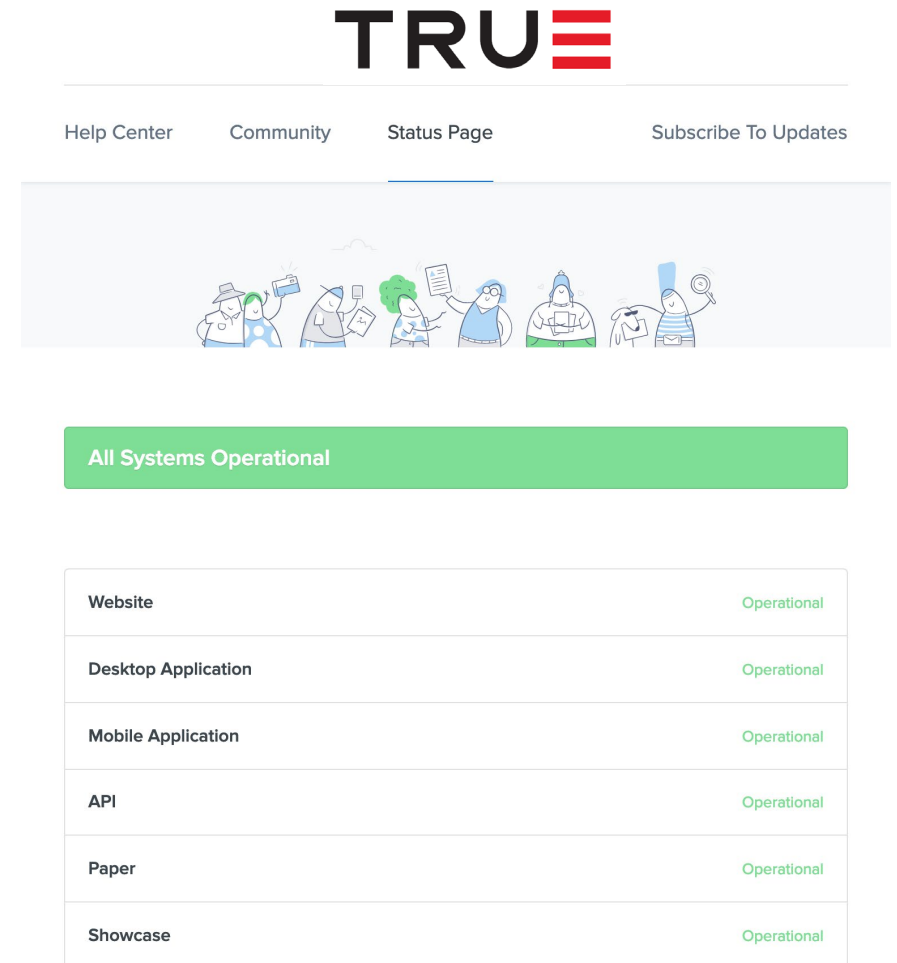
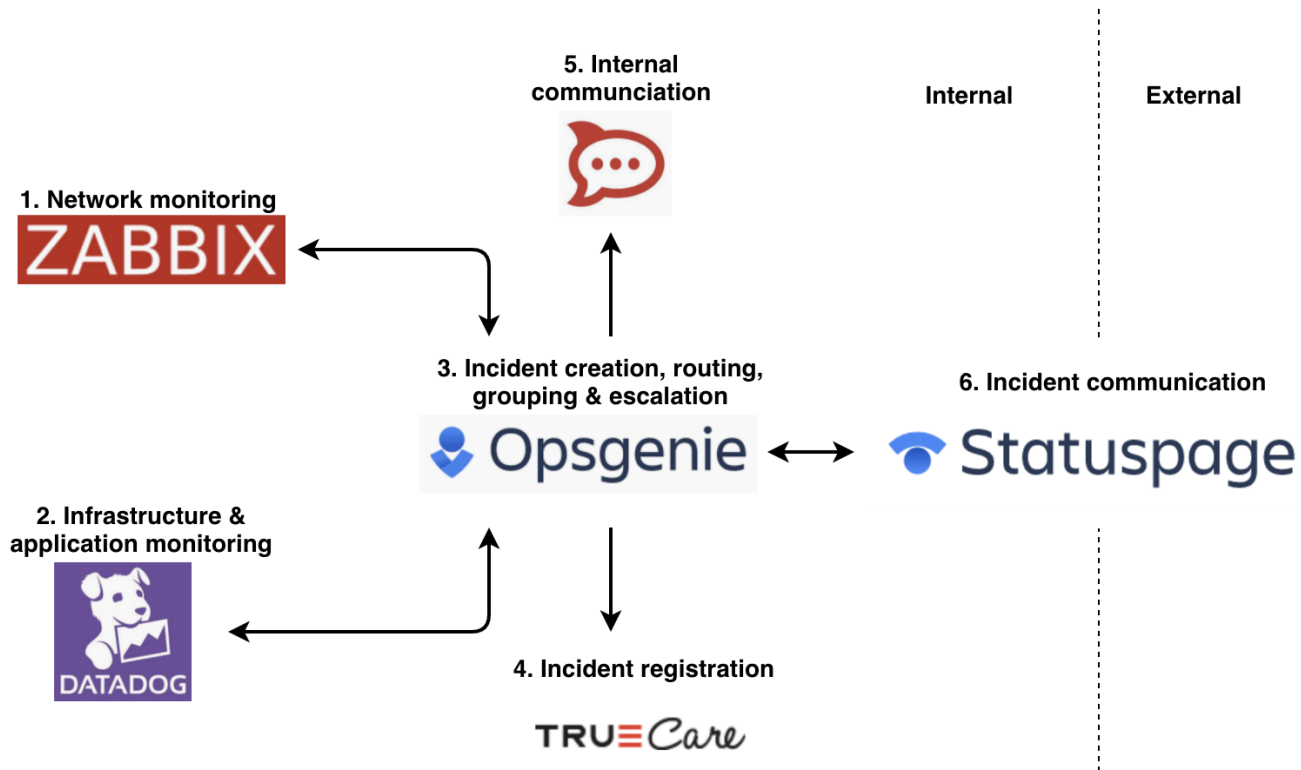
2020-01-31
15:06:53
oec (OpsGenie OEC)



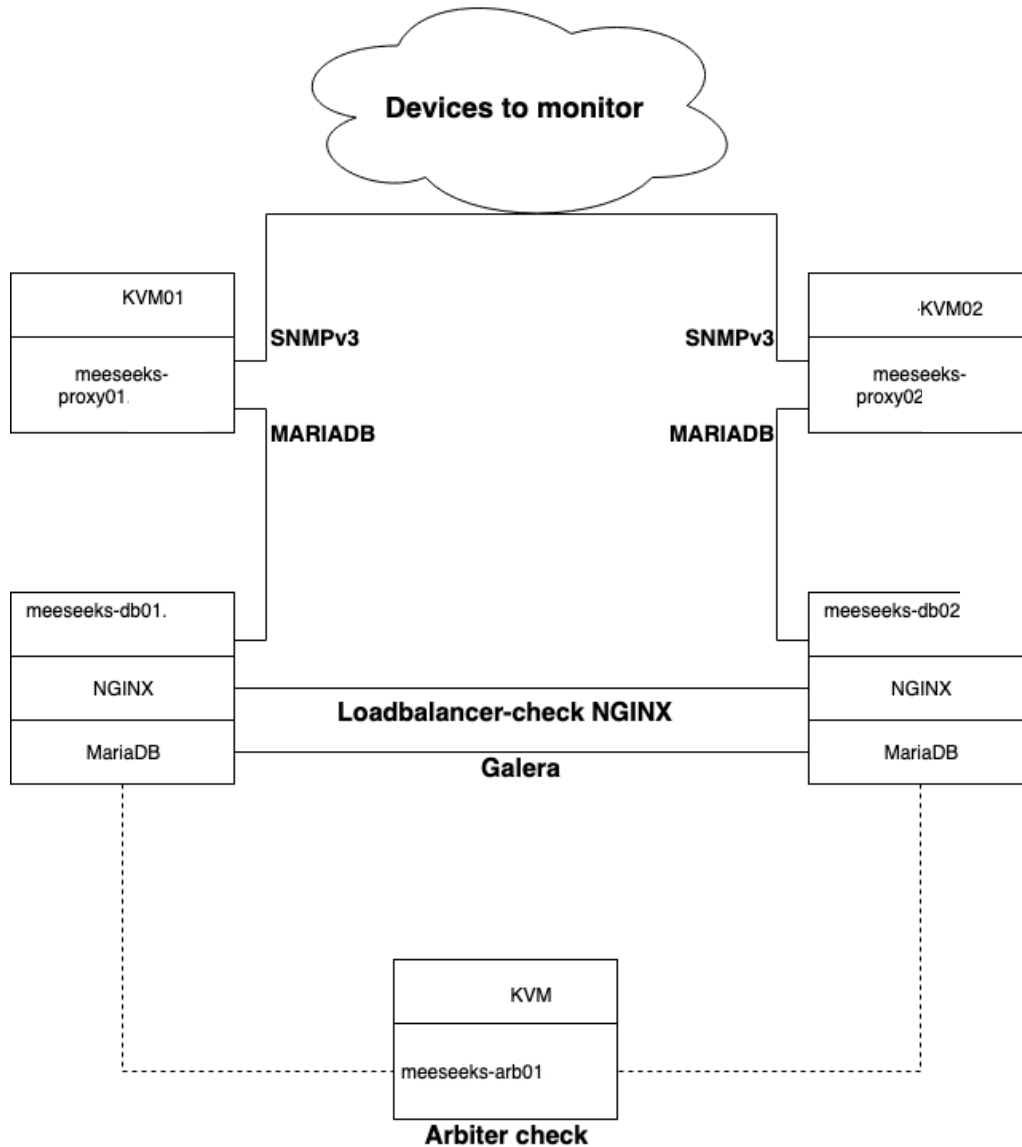
Acknowledged by Zabbix via Opsgenie

Future

- Datadog -> Zabbix (if allowed...)
- Statuspage



Future



- Proxy off-loading
- Redundancy

Thank you

Questions?

