



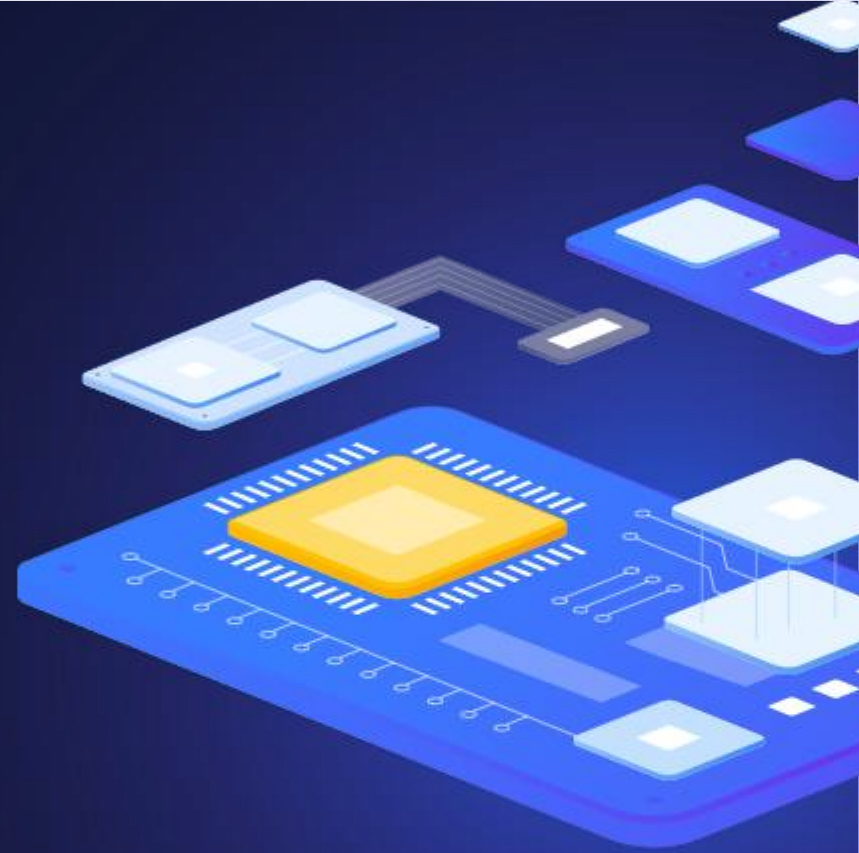
Webinar

Advanced problem detection

all our microphones are muted

ask your questions in Q&A, not in the Chat

use Chat for discussion, networking or applause

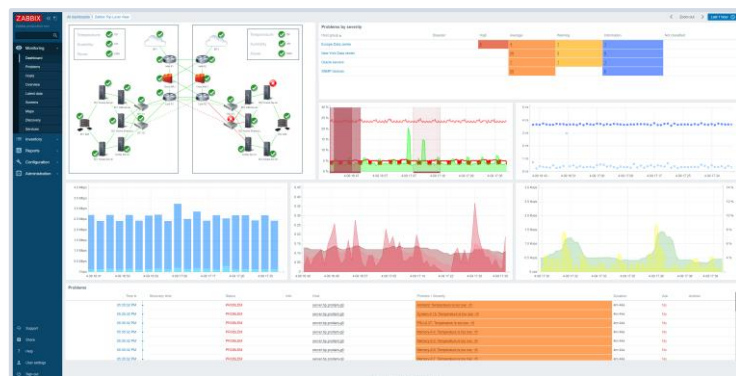


1

Zabbix data flow

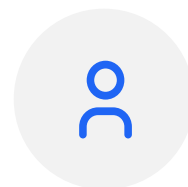
ADVANCED PROBLEM DETECTION

Zabbix data flow



Visualization

Notifications



DATABASE

ZABBIX SERVER

History

Analysis

Data collection



ADVANCED PROBLEM DETECTION

How often to execute checks?

Every N seconds

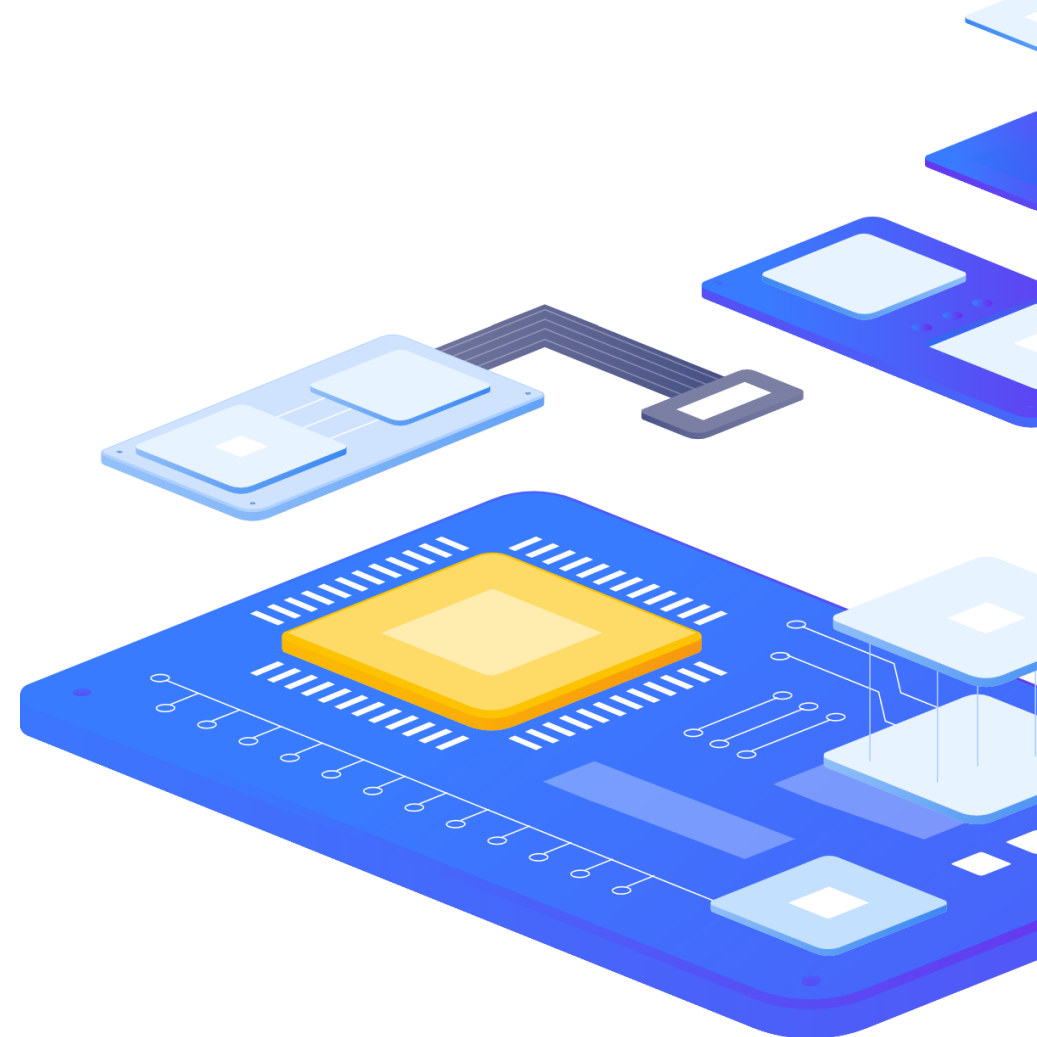
- › Zabbix will evenly distribute checks

Different frequency in different time periods

- › Every X seconds in working time
- › Every Y second in weekend

At a specific time (Zabbix 3.0)

- › Ready for business checks
- › Every hour starting from 9:00 at working hours (9:00, 10:00, ..., 18:00)



2

Triggers



Trigger – problem definition

Example

- › `last(/server/system.cpu.load) > 5`

Operators

- › `- + / * < > = <> >= <= not or and`

Functions

- › `min max avg last count date time diff regexp` and much more!

Analyze everything: any metric and any host

- › `last(/node1/system.cpu.load) > 5 and last(/node2/system.cpu.load) > 5 and last(/nodes/tps) < 5000`

Trigger Functions

Function group	Functions
Aggregate functions	avg, bucket_percentile, count, histogram_quantile, item_count, kurtosis, mad, max, min, skewness, stddevpop, stddevsamp, sum, sumofsquares, varpop, varsamp
Bitwise functions	bitand, bitlshift, bitnot, bitor, bitrshift, bitxor
Date and time functions	date, dayofmonth, dayofweek, now, time
History functions	baselinedev, baselinewma, change, changecount, count, countunique, find, first, fuzzytime, last, logeventid, logseverity, logsource, monodec, monoinc, nodata, percentile, rate, trendavg, trendcount, trendmax, trendmin, trendstl, trendsum
Mathematical functions	abs, acos, asin, atan, atan2, avg, cbrt, ceil, cos, cosh, cot, degrees, e, exp, expm1, floor, log, log10, max, min, mod, pi, power, radians, rand, round, signum, sin, sinh, sqrt, sum, tan, truncate
Operator functions	between, in
Prediction functions	forecast, timeleft
String functions	ascii, bitlength, bytelength, char, concat, insert, left, length, ltrim, mid, repeat, replace, right, rtrim, trim

Foreach Functions - tip

- › avg_foreach
- › bucket_rate_foreach
- › count_foreach
- › exists_foreach
- › last_foreach
- › max_foreach
- › min_foreach
- › sum_foreach

Calculated Items on:

Host level

- › `sum(last_foreach(/host/net.if.in[*]))`

Hostgroup level

- › `avg_foreach(/*/mysql.qps?[group="MySQL Servers"],5m)`

ADVANCED PROBLEM DETECTION

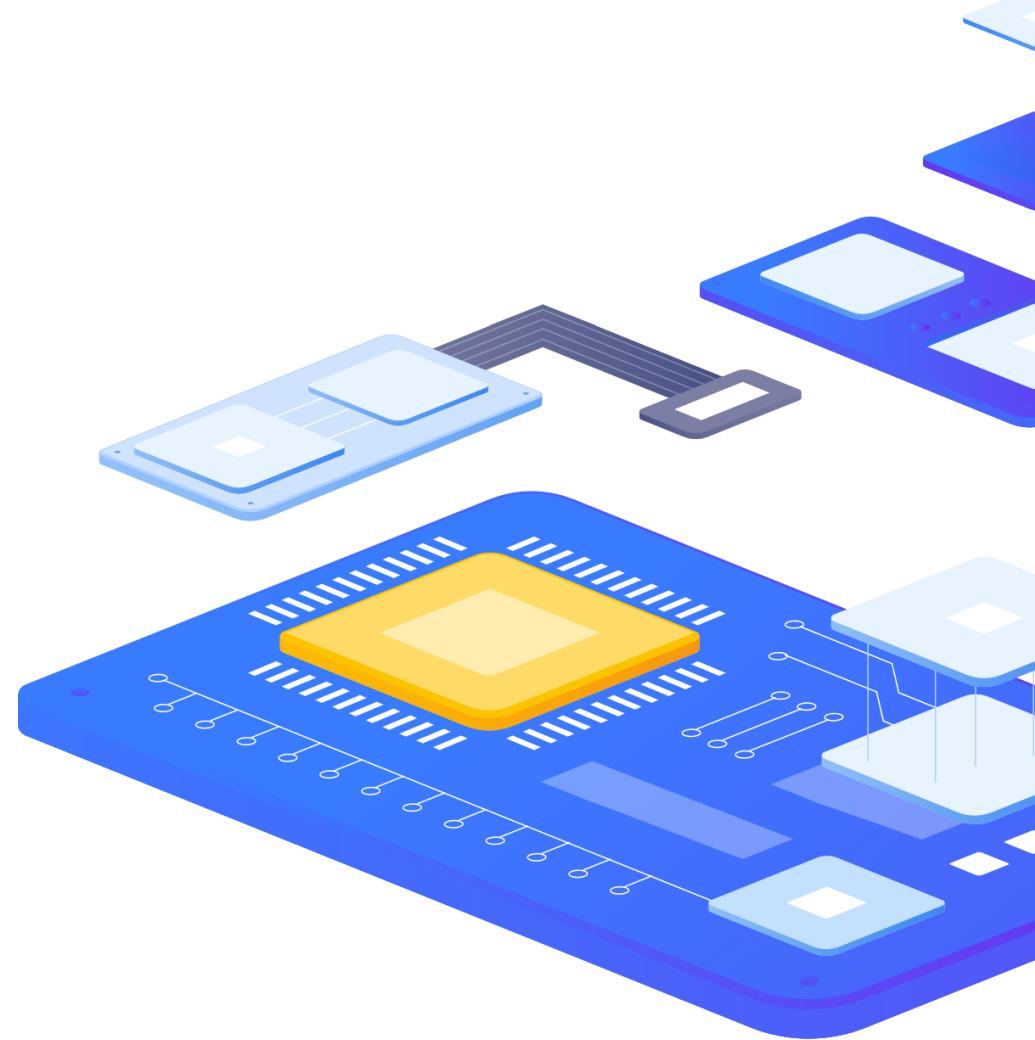
Junior level

Performance

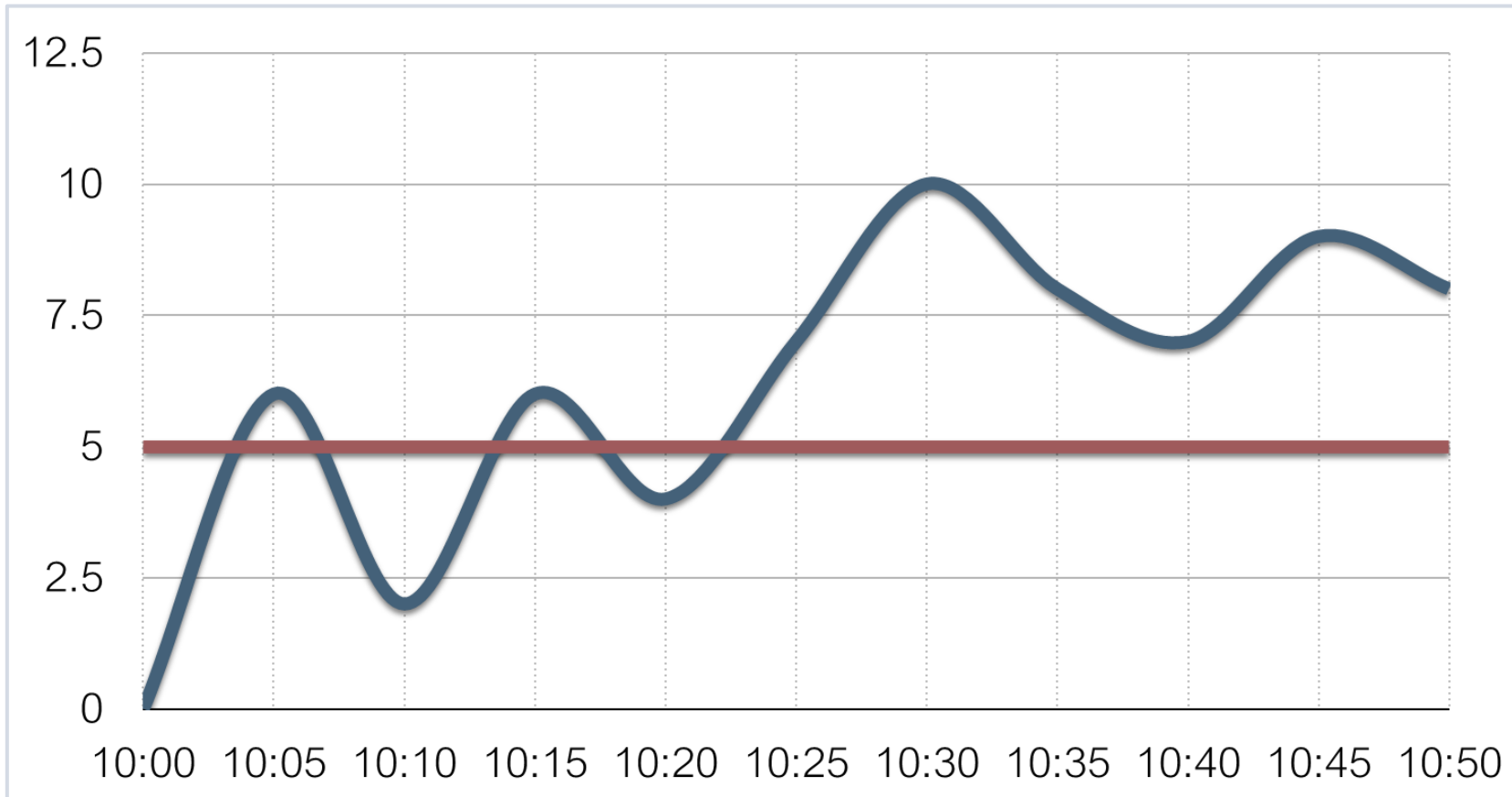
- › `last(/server/system.cpu.load) > 5`

Availability

- › `last(/server/net.tcp.service[http]) = 0`



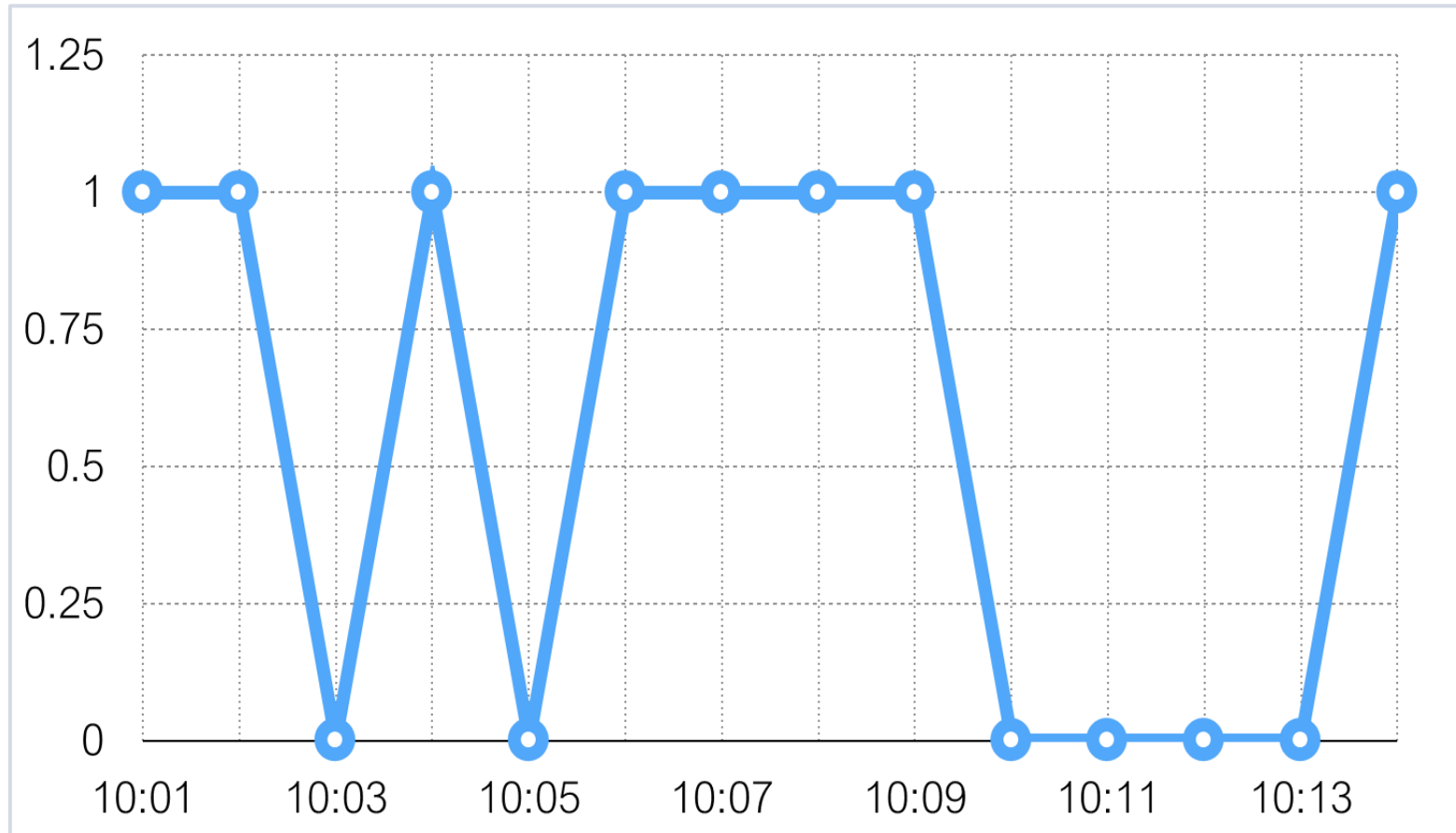
False positives



```
last(/server/system.cpu.load) > 5
```

ADVANCED PROBLEM DETECTION

Too sensitive

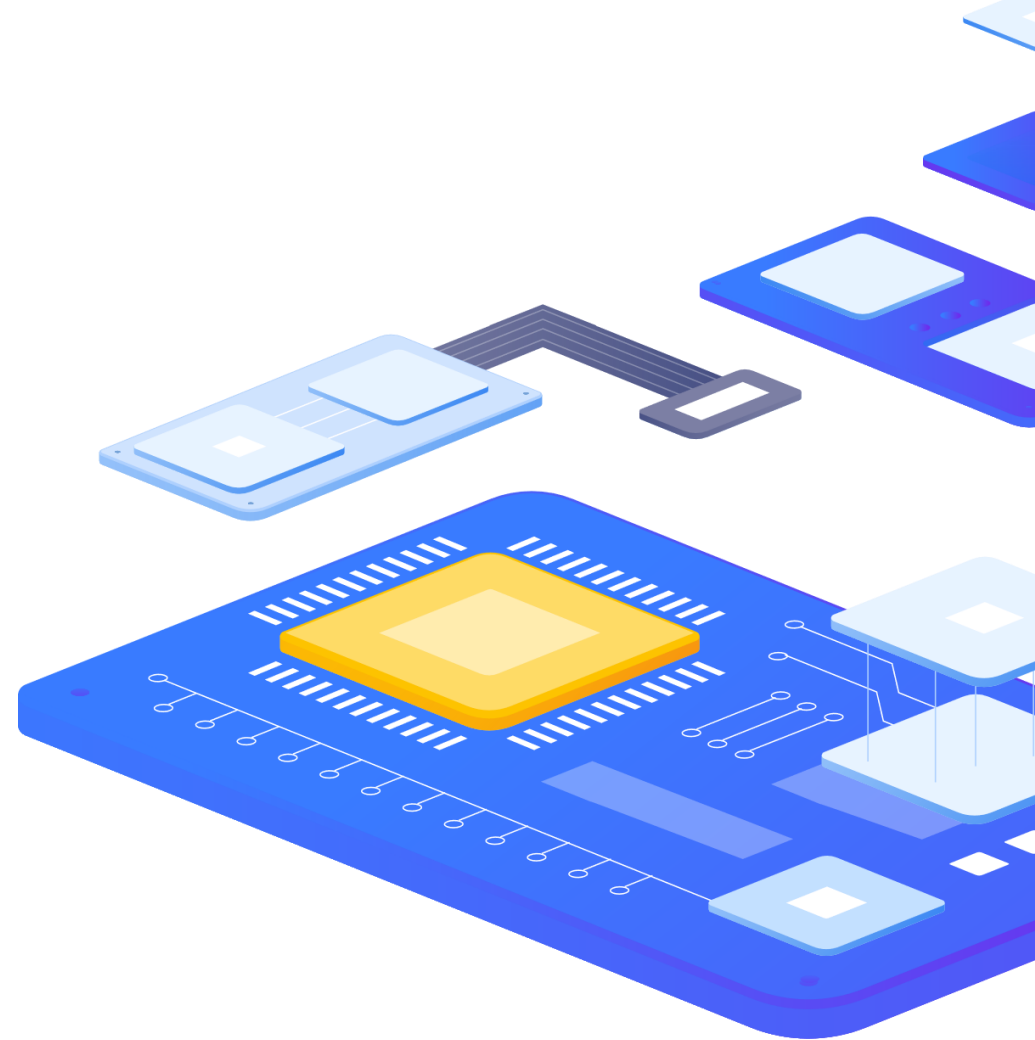


`last(/server/net.tcp.service[http]) = 0`

Junior level

Too sensitive leads to

- ▶ False positives



3

False positives



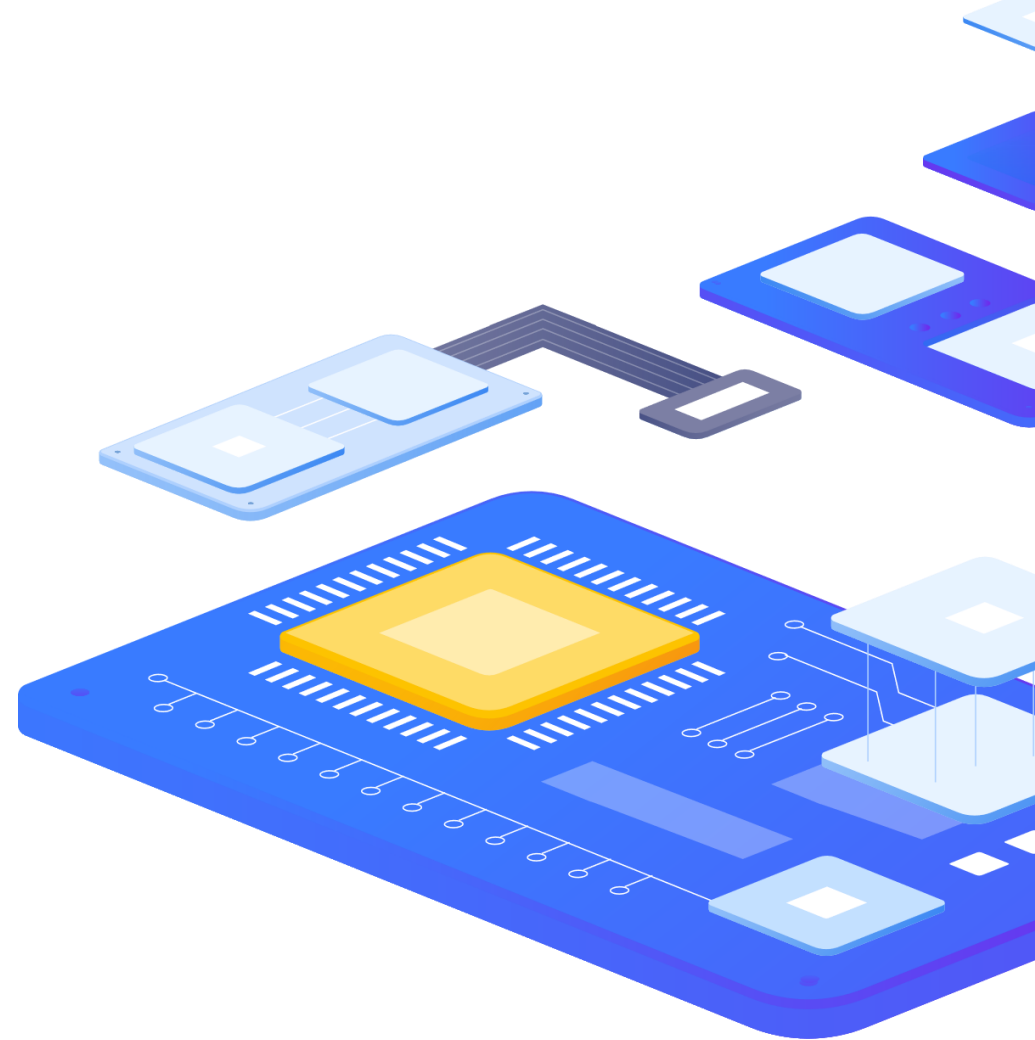
ADVANCED PROBLEM DETECTION

How to avoid false positives?

Be careful and define problems wisely!

What does it really mean?

- › system is overloaded
- › application does not work
- › service is not available



ADVANCED PROBLEM DETECTION

Examples

Problem:

- › CPU load > 5

No problem:

- › CPU load = 4.99 → Resolved?

Problem:

- › free disk space < 10%

No problem:

- › free disk space = 10.001% → Resolved?

Problem:

- › SSH check failed

No problem:

SSH is up → Resolved?

Analyze history

Performance

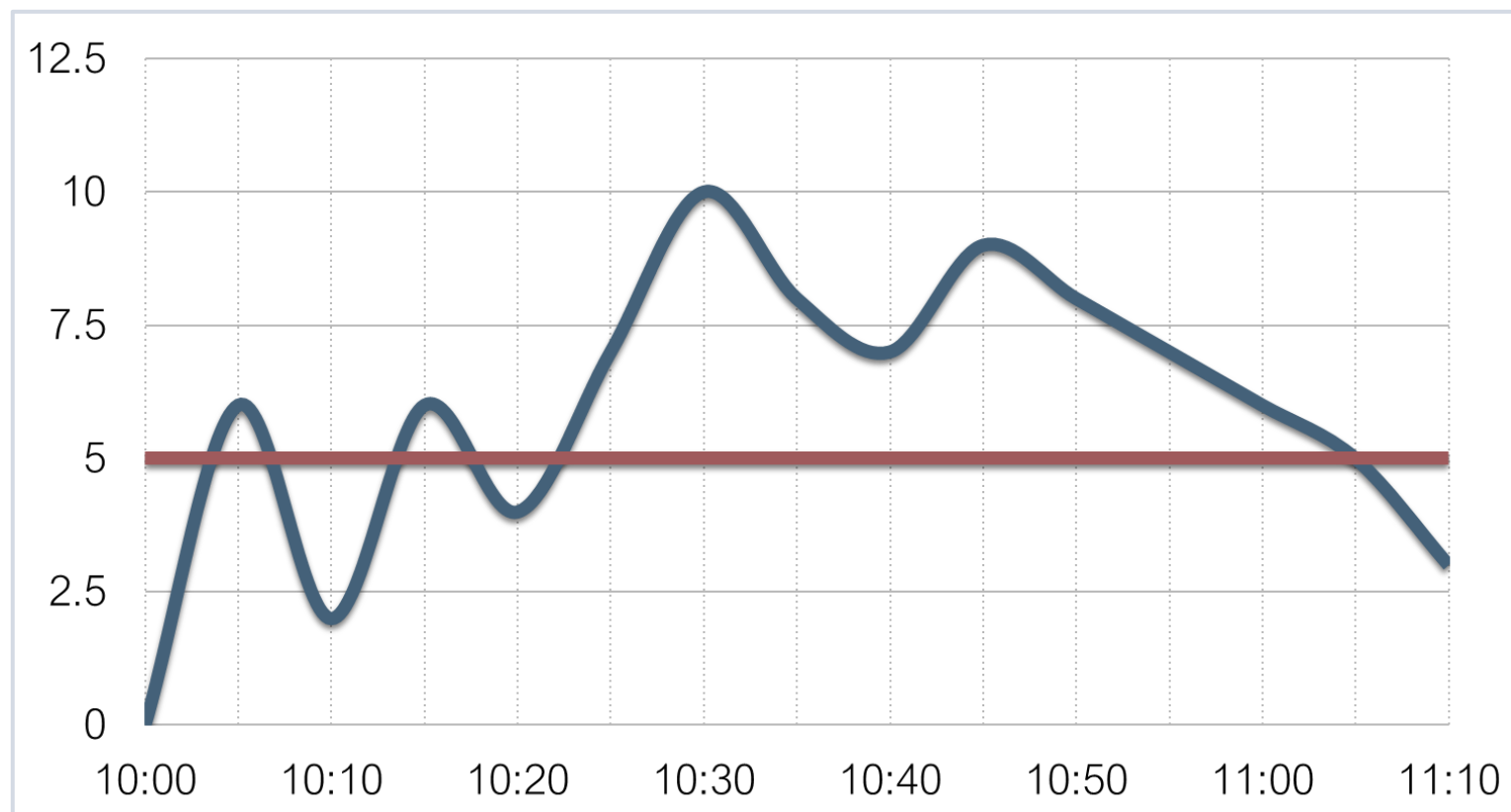
- › $\min(/server/system.cpu.load,10m) > 5$

Availability

- › $\max(/server/net.tcp.service[http],5m) = 0$
- › $\max(/server/net.tcp.service[http],\#3) = 0$

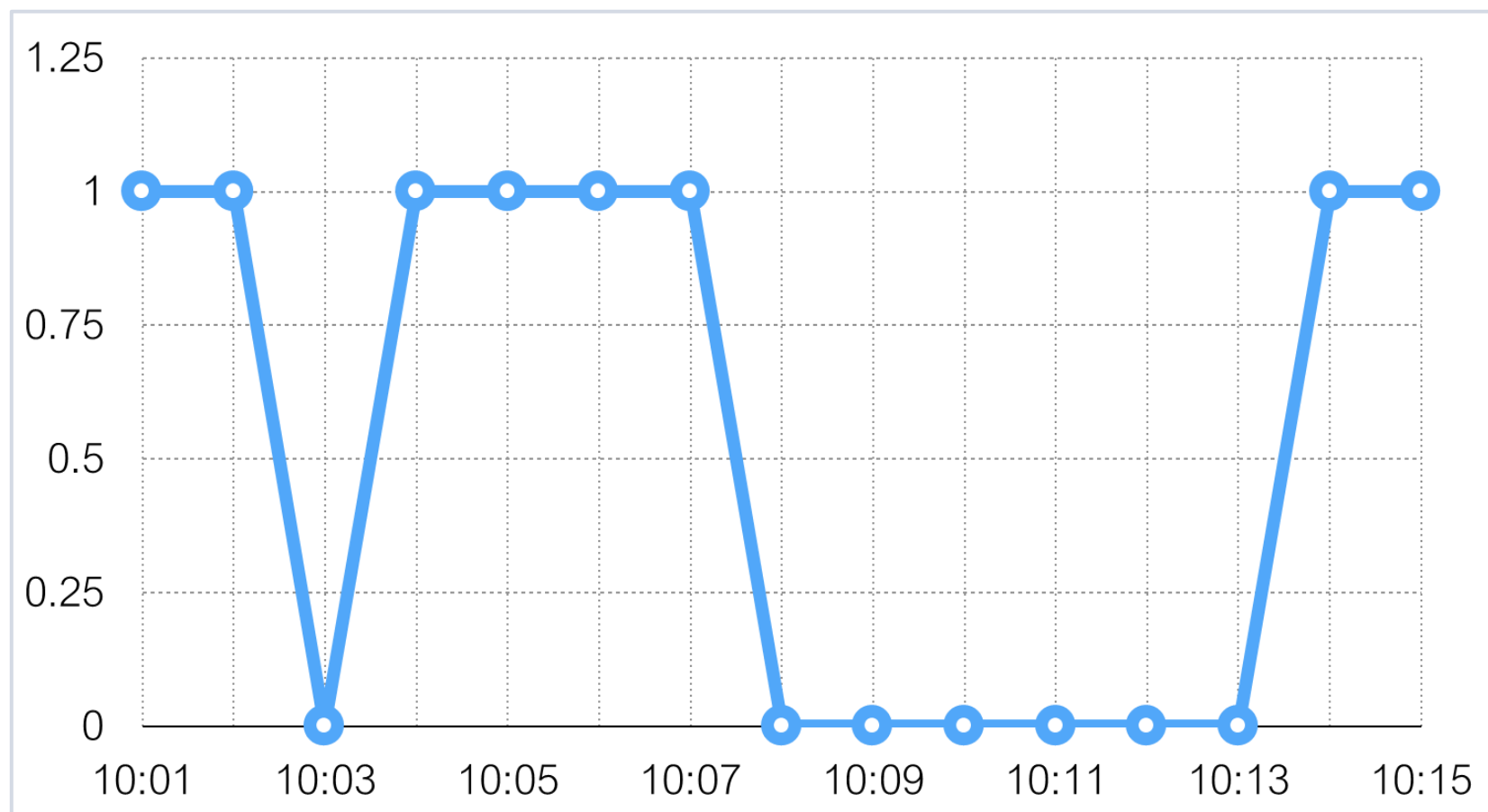
ADVANCED PROBLEM DETECTION

Analyze history



```
min(/server/system.cpu.load,10m) > 5
```

Analyze history



`max(/server/net.tcp.service[http],#3) = 0`

Different conditions for problem and recovery

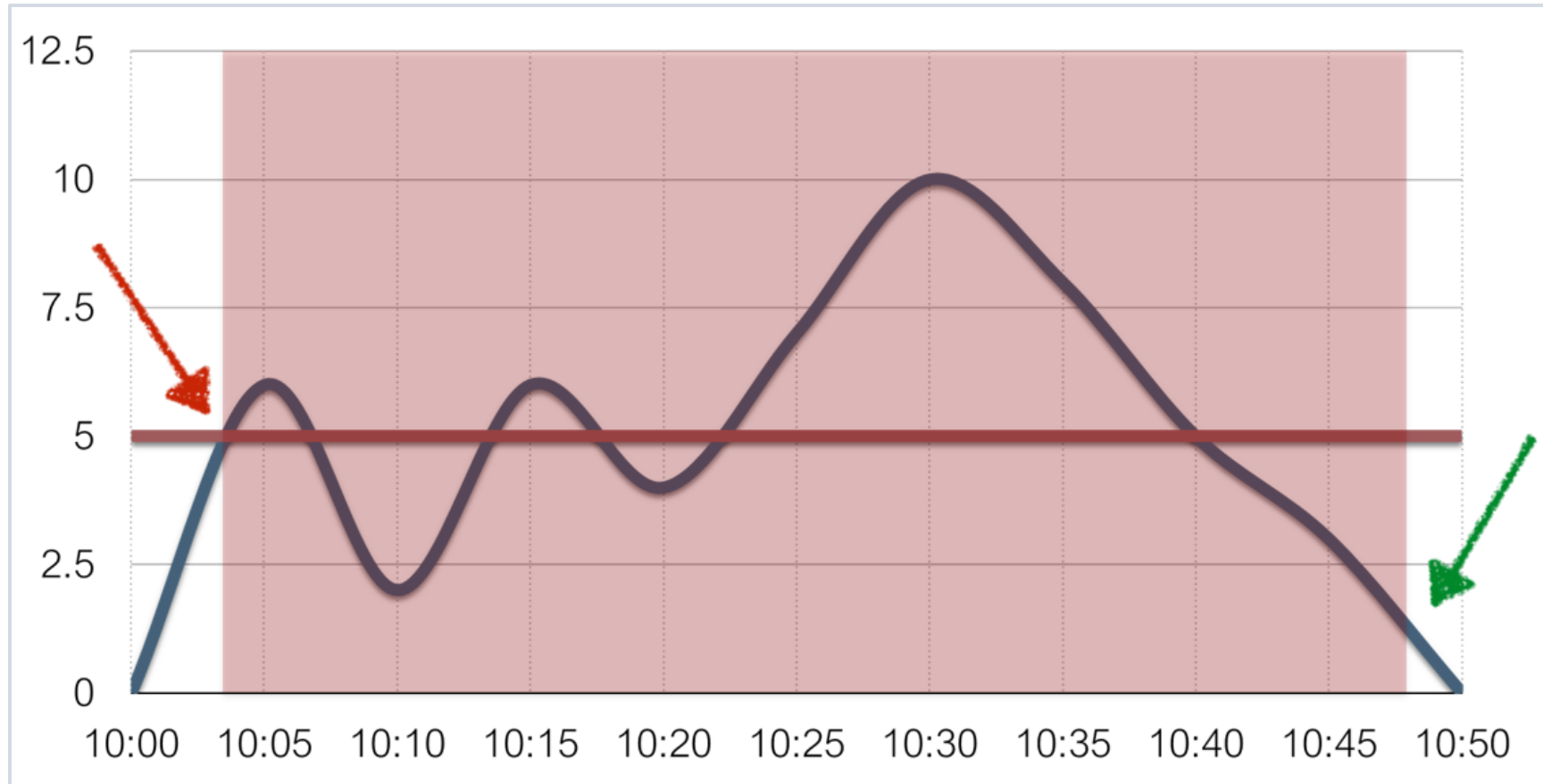
Before

- › `last(/server/system.cpu.load) > 5`

Now

- › Problem definition: `last(/server/system.cpu.load)>5`
- › Recovery expression: `last(/server/system.cpu.load)}<=1`

Different conditions for problem and recovery



Problem definition: `last(/server/system.cpu.load)>5` ...Recovery expression: `last(/server/system.cpu.load)}<=1`

Examples

System is overloaded

Problem definition:

- › $\min(/server/system.cpu.load,5m)>3$

Recovery expression:

- › $\max(/server/system.cpu.load,2m)\leq 1$

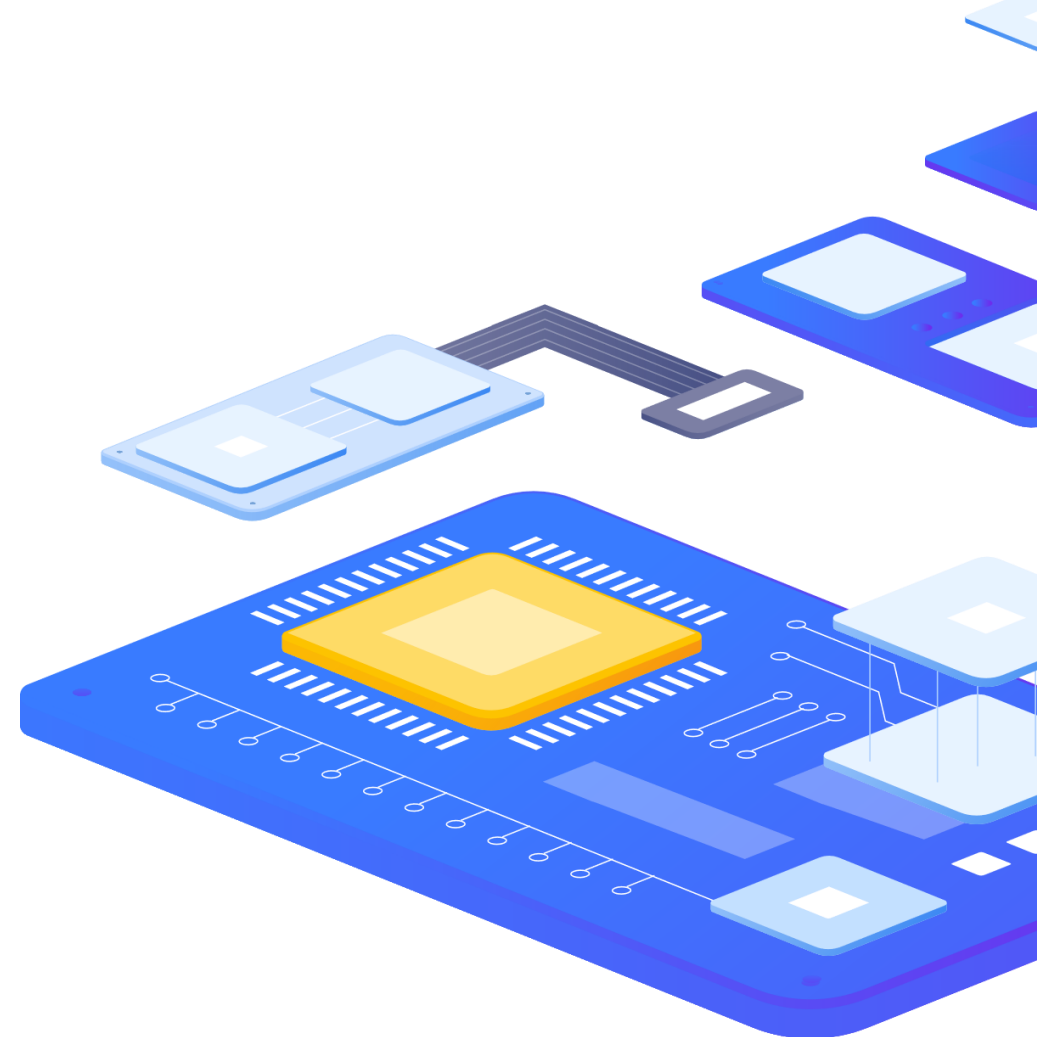
No free disk space /

Problem definition:

- › $\text{last}(/server/vfs.fs.size[/,pfree])<10$

Recovery expression:

- › $\min(/server/vfs.fs.size[/,pfree],15m)>30$



Examples

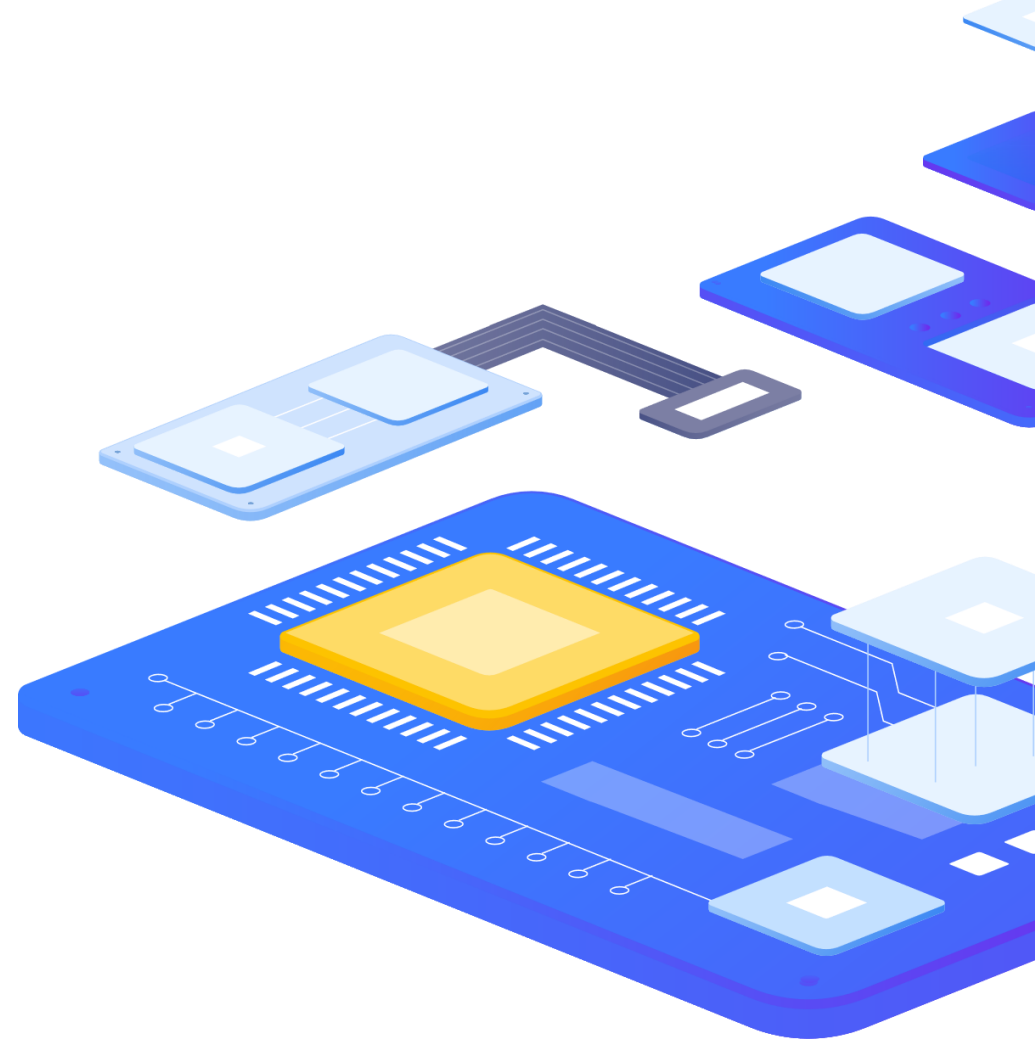
SSH is not available

Problem definition:

› $\max(/server/net.tcp.service[ssh],\#3)=0$

Recovery expression:

› $\min(/server/net.tcp.service[ssh],\#10)=1$



Anomalies

How to detect?

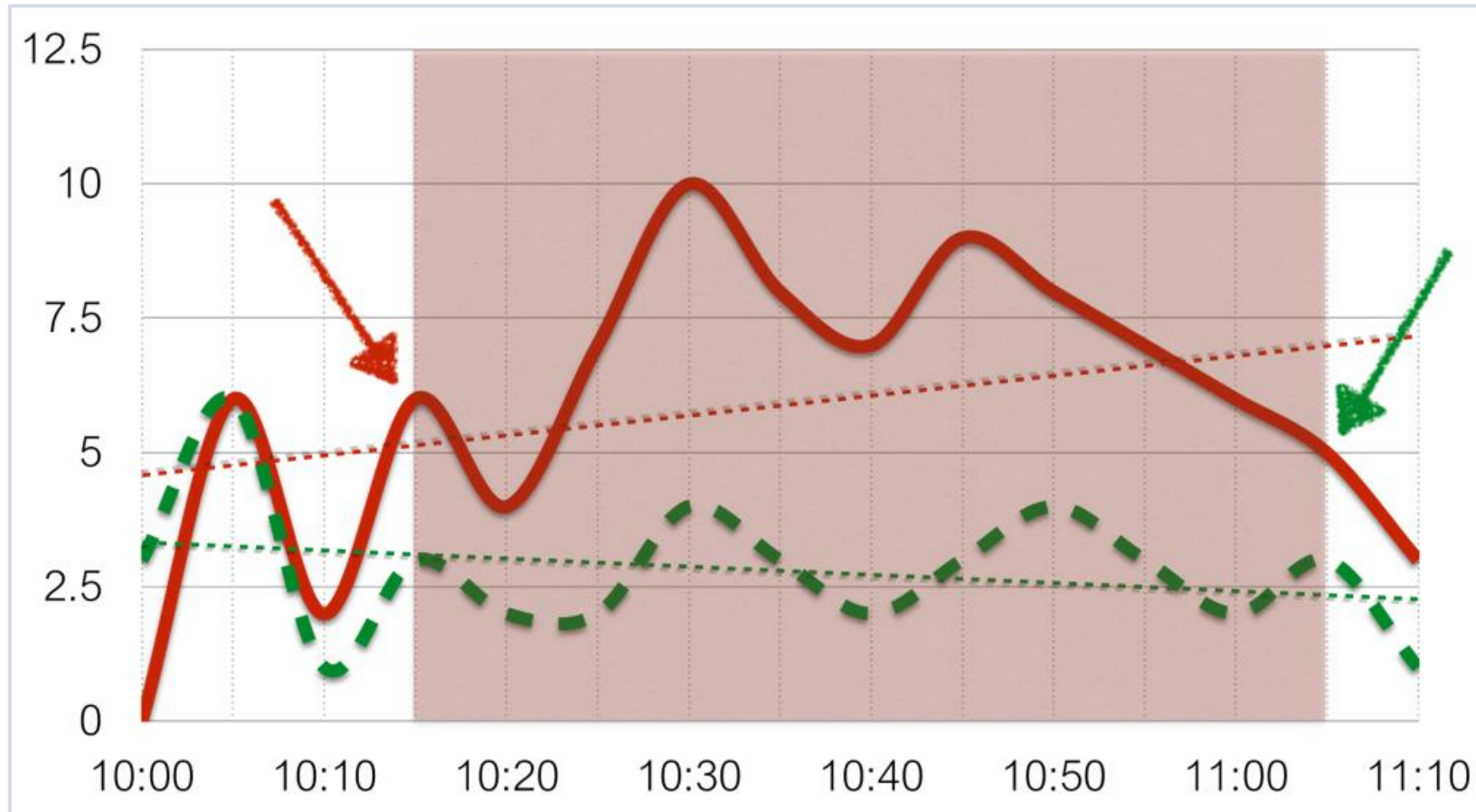
By comparing with the data from the same period, the period is taken from the past.

Average CPU load for the last hour is 2x higher than

CPU load for the same period week ago

▶ `avg(/server/system.cpu.load,1h) > 2* avg(/server/system.cpu.load,1h:now-1w)`

Anomalies



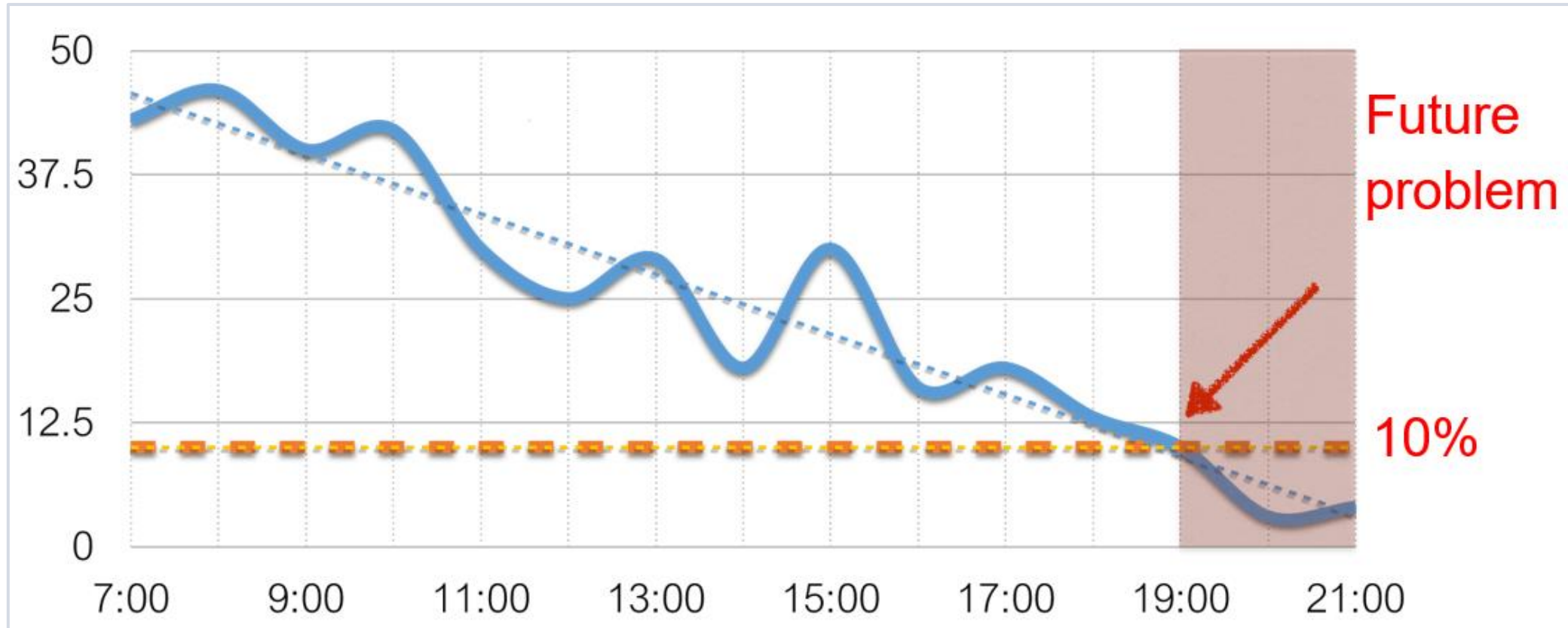
Comparison with the data 7 days ago

3

Forecast

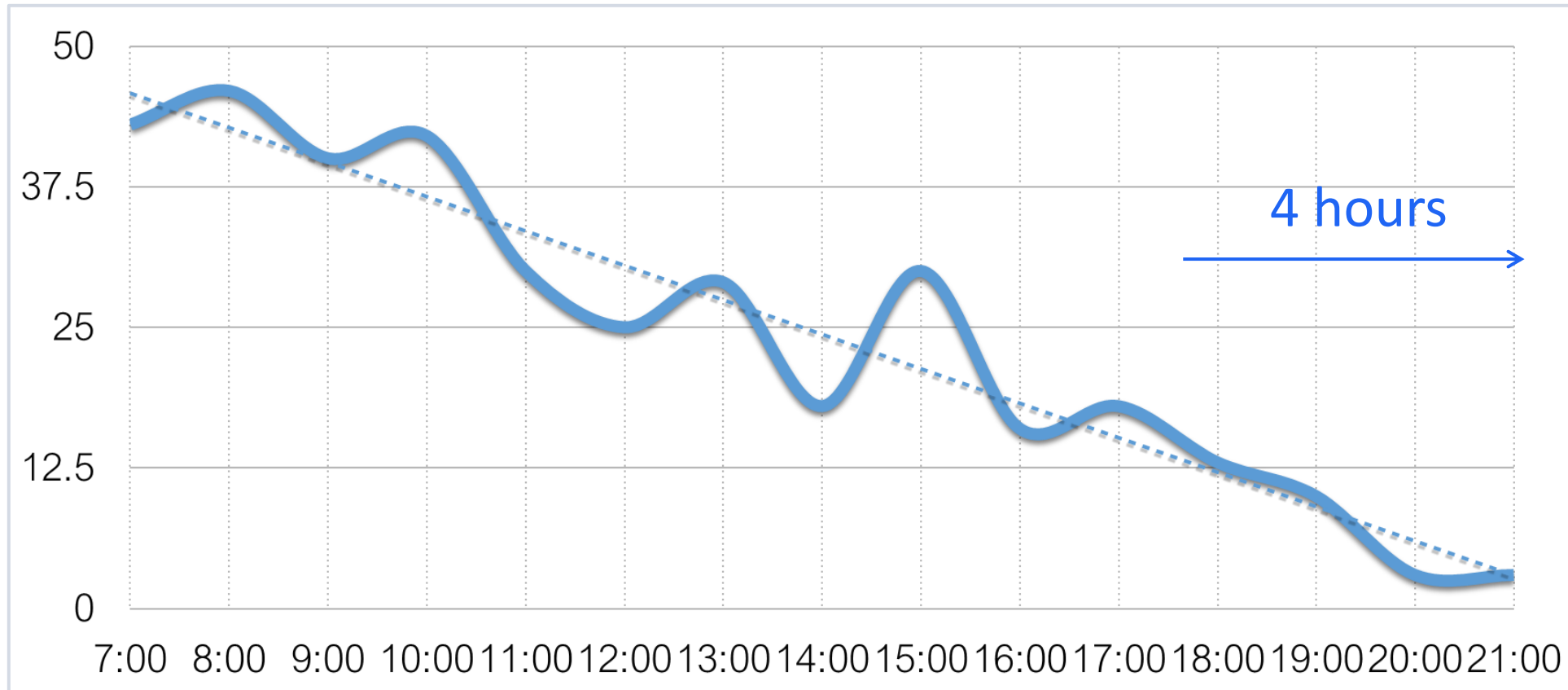


Forecast



Trigger function timeleft

Forecast

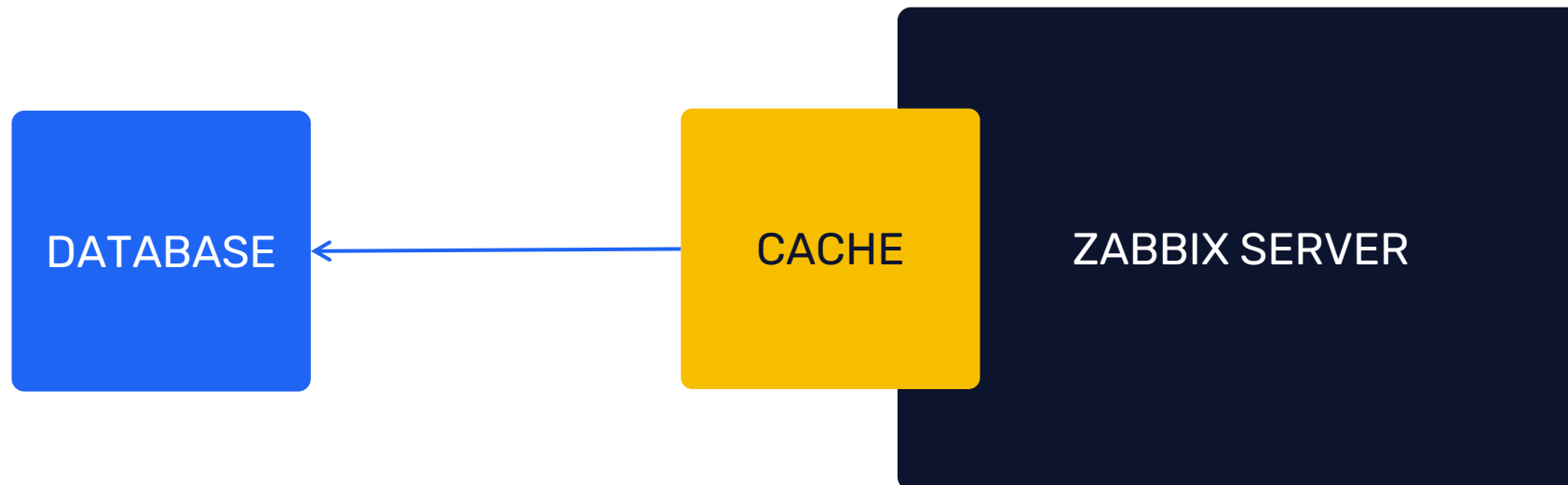


Trigger function forecast

Does history analysis affect performance of Zabbix?

Yes, but not significantly.

Especially as of Zabbix 2.2.0.



4

Dependencies



Dependencies

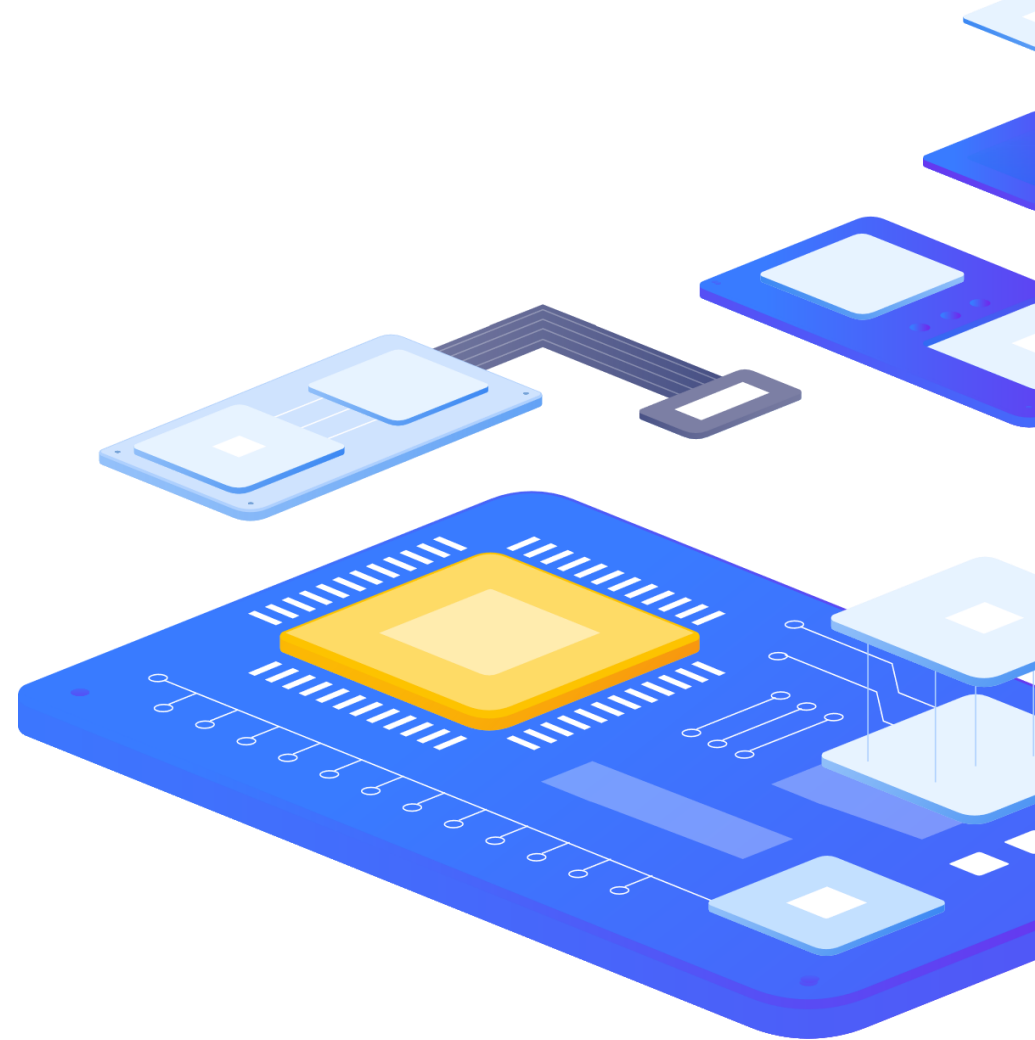
CRM is not working



DB is unavailable



No free disk space



ADVANCED PROBLEM DETECTION

Section „Problems“

initMAX <<

Problems
Export to CSV

Show: Recent problems | Problems | History

Host groups: Select

Hosts: Select

Application: Select

Triggers: Select

Problem:

Severity:
 Not classified
 Information
 Average
 Warning
 High
 Disaster

Age less than: days

Host inventory: Type Remove

Add

Tags: And/Or Or

Contains Equals value Remove

Add

Show tags: None 1 2 3 Tag name Full Shortened None

Tag display priority:

Show operational data: None Separately With problem name

Show suppressed problems: Show unacknowledged only

Compact view: Show timeline

Show details: Highlight whole row

Apply Reset

Time	Severity	Info	Host	Problem	Duration	Ack	Actions	Tags
05:35:32 PM	Information		server.hp.proliant-c9	CPU-0.3: Temperature is too low: <5	9m 35s	No		
05:35:32 PM	Information		server.hp.proliant-c9	CPU-0.2: Temperature is too low: <5	9m 35s	No		
05:35:31 PM	Information		server.hp.ilo	CPU-0.2: Temperature is too low: <5	9m 36s	No		
03:06:07 PM	Warning		net.mikrotik.rp1100ah	↓ Device: Temperature is above warning threshold: >60	2h 39m	No		
03:54:06 AM	High		net.mikrotik.450g	↑ Device: Temperature is above critical threshold: >60	13h 51m 1s	No	🔧	Cloud: No Service: Network
04/03/2020 07:56:11 AM	Warning		DatabaseX	↓ Disk space is low (used ≥ 80%)	6d 5h 48m	No		
04/03/2020 07:56:07 AM	Warning		Zabbix server	↓ Disk space is low (used ≥ 80%)	6d 5h 49m	No		
04/03/2020 07:56:52 AM	Warning		demo1.zabbix.lan	↓ Disk space is low (used ≥ 80%)	6d 5h 49m	No		
04/03/2020 07:55:24 AM	Warning		Windows2008	Free disk space is less than 20% on volume:	6d 5h 49m	No	🔧	Class: Storage Monitoring: Discovery
04/03/2020 07:42:31 AM	Information		DatabaseX	↑ Operating system description has changed	6d 10h 2m	No		
04/03/2020 07:31:12 AM	Information		Zabbix server	↑ Operating system description has changed	6d 10h 13m	No		
04/03/2020 07:11:40 AM	Information		net.mikrotik.912UAG-5HPrD	↓ Interface eth0/1: Ethernet has changed to lower speed than it was before	6d 10h 33m	No		Environment: DEV
04/03/2020 04:00:06 AM	High		net.mikrotik.450g	↑ Device: Temperature is above critical threshold: >60	6d 13h 45m	No	🔧	Cloud: No Service: Network
04/02/2020 08:21:06 PM	High		net.mikrotik.450g	↑ Device: Temperature is above critical threshold: >60	6d 21h 24m	No	🔧	Cloud: No Service: Network
03/31/2020 09:13:55 AM	Warning		Testing JMX Template	mp.SurvivorSpace:fully.committed on Testing JMX Template	9d 8h 31m	No		Application: JAVA
03/13/2020 05:20:46 PM	Information		Switch HP 2530-45g	↓ Interface 12(i): Ethernet has changed to lower speed than it was before	27d 24m	No		Environment: DEV
03/13/2020 04:40:46 PM	Information		Switch HP 2530-45g	↓ Interface 29(i): Ethernet has changed to lower speed than it was before	27d 1h 4m	No		Environment: DEV
03/13/2020 03:56:46 PM	Information		Switch HP 2530-45g	↓ Interface 41(i): Ethernet has changed to lower speed than it was before	27d 1h 49m	No		Environment: DEV
03/13/2020 03:25:46 PM	Information		Switch HP 2530-45g	↓ Interface 11(i): Ethernet has changed to lower speed than it was before	27d 2h 19m	No		Environment: DEV
02/21/2020 07:20:46 AM	Information		Switch HP 2530-45g	↓ Interface 45(i): Ethernet has changed to lower speed than it was before	1m 18d 10h	No		Environment: DEV
02/12/2020 04:16:32 PM	High		server.hp.proliant-c9	↑ Slot 2: Disk array controller is in critical state	1m 27d 1h	No		
02/11/2020 04:30:08 PM	Warning		Oracle Database 01 (11g Express)	System time is out of sync (diff with Zabbix server > 60s)	1m 28d 1h	Yes	🔧	
01/16/2020 12:33:00 PM	Warning		MySQL Host	↓ MySQL: Failed to get theme (no data for 30m)	2m 24d 5h	No		
10/09/2019 09:12:27 AM	Information		pci.brocade.fc_300_2	↓ SLOT #0: TEMP #3: Temperature is above warning threshold: >65	1y 6m 3d	Yes	🔧	

5

Tags



Tags

Tag word: meaning

Customer: Alza

Customer: Globus

Datacenter: NY2

Datacenter: San Francisco

Area: Performance

Area: Availability

Area: Security

Environment: Staging

Environment: Test

User impact: None

User impact: Critical

ADVANCED PROBLEM DETECTION

Use of obtained values

Use of useful information in tags or names

* Name	Free disk space is less than {\$LOW_SPACE_PCT_HIGH:"{#FSNAME}"}% on volur
Event name	Free disk space is less than {\$LOW_SPACE_PCT_HIGH:"{#FSNAME}"}% on volume {#FSNAME}
Operational data	{ITEM.LASTVALUE1} (Total: {ITEM.LASTVALUE2}, Free: {ITEM.LASTVALUE3})
Severity	<input type="checkbox"/> Not classified <input type="checkbox"/> Information <input type="checkbox"/> Warning <input type="checkbox"/> Average <input checked="" type="checkbox"/> High <input type="checkbox"/> Disaster
* Expression	<pre>last(/Template OS - Windows - za/vfs.fs.size[{#FSNAME},pfree]) <{\$LOW_SPACE_PCT_HIGH:"{#FSNAME}"} and last(/Template OS - Windows - za/vfs.fs.size[{#FSNAME},total])>=0 and last(/Template OS - Windows - za/vfs.fs.size[{#FSNAME},free])>=0</pre> Add
	Expression constructor
OK event generation	<input checked="" type="checkbox"/> Expression <input type="checkbox"/> Recovery expression <input type="checkbox"/> None

Possible reactions

- › Event correlation
- › Automatized problem solving
- › Manual problem closing
- › Sending notifications to a user or a group of users
- › Registration of tasks in the Helpdesk system

6

Event correlations



Event correlation on trigger level

Trigger **Tags** Dependencies

Name Service `{{ITEM.VALUE}.regsub("^.* service ([a-zA-Z]*) .*$", "\1")}` stopped

Event name Service `{{ITEM.VALUE}.regsub("^.* service ([a-zA-Z]*) .*$", "\1")}` stopped

Operational data

Severity Not classified Information Warning Average High Disas

Problem expression `find(/My host/log[/var /log/syslog],, "regexp", "Stopping")=1`

[Expression constructor](#)

OK event generation Expression Recovery expression None

Recovery expression `find(/My host/log[/var /log/syslog],, "regexp", "Starting")=1`

[Expression constructor](#)

PROBLEM event generation mode Single Multiple

OK event closes All problems All problems if tag values match

Tag for matching Service

Correlation of events at the trigger level allows you to compare individual problems reported by a single trigger.

Trigger **Tags 2** Dependencies

Trigger tags Inherited and trigger tags

Name	Value
Datcenter	value
Service	<code>{{ITEM.VALUE}.regsub("^.* service ([a-zA-Z]*) .*\$", "\1")}</code>

[Add](#)

Event correlation on trigger level

How does it work?

10/Feb/2022:06:25:30 service Jira stopped

“Service Jira stopped”

PROBLEM

Event correlation on trigger level

How does it work?

10/Feb/2022:06:25:30 service Jira stopped "Service Jira stopped" **PROBLEM**

10/Feb/2022:06:27:32 service MySQL stopped "Service MySQL stopped" **PROBLEM**

Event correlation on trigger level

How does it work?

10/Feb/2022:06:25:30 service Jira stopped	"Service Jira stopped"	PROBLEM
10/Feb/2022:06:27:32 service MySQL stopped	"Service MySQL stopped"	RESOLVED
10/Feb/2022:06:28:11 service MySQL started		

ADVANCED PROBLEM DETECTION

Event correlation on trigger level

How does it work?

10/Feb/2022:06:25:30	service Jira stopped	"Service Jira stopped"	PROBLEM
10/Feb/2022:06:27:32	service MySQL stopped	"Service MySQL stopped"	RESOLVED
10/Feb/2022:06:28:11	service MySQL started		
10/Feb/2022:06:34:22	service Redis stopped	"Service Redis stopped"	PROBLEM

ADVANCED PROBLEM DETECTION

Event correlation on trigger level

How does it work?

10/Feb/2022:06:25:30 service Jira stopped	"Service Jira stopped"	PROBLEM
10/Feb/2022:06:27:32 service MySQL stopped	"Service MySQL stopped"	RESOLVED
10/Feb/2022:06:28:11 service MySQL started		
10/Feb/2022:06:34:22 service Redis stopped	"Service Redis stopped"	RESOLVED
10/Feb/2022:06:37:58 service Redis started		

ADVANCED PROBLEM DETECTION

Event correlation on trigger level

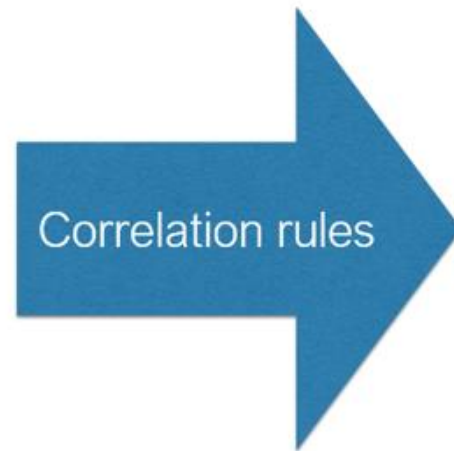
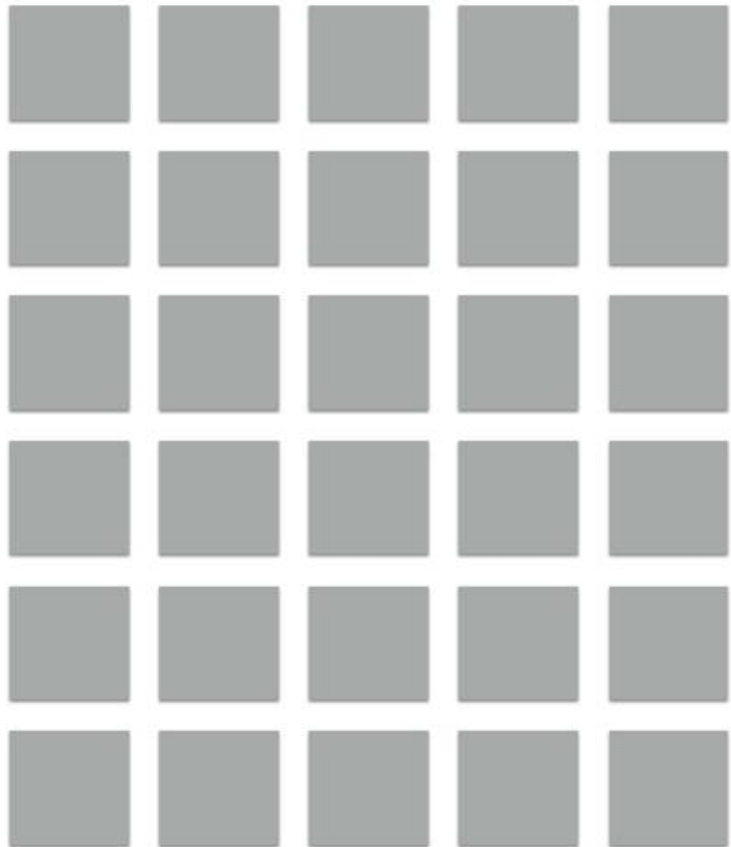
How does it work?

10/Feb/2022:06:25:30 service Jira stopped	"Service Jira stopped"	RESOLVED
10/Feb/2022:06:27:32 service MySQL stopped	"Service MySQL stopped"	RESOLVED
10/Feb/2022:06:28:11 service MySQL started		
10/Feb/2022:06:34:22 service Redis stopped	"Service Redis stopped"	RESOLVED
10/Feb/2022:06:37:58 service Redis started		
10/Feb/2022:06:55:31 service Jira started		

Event correlation

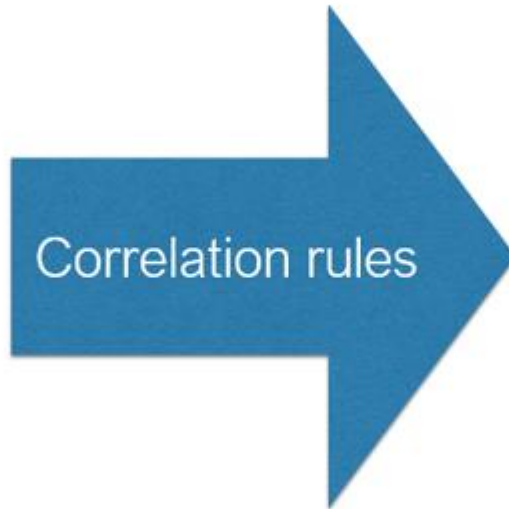
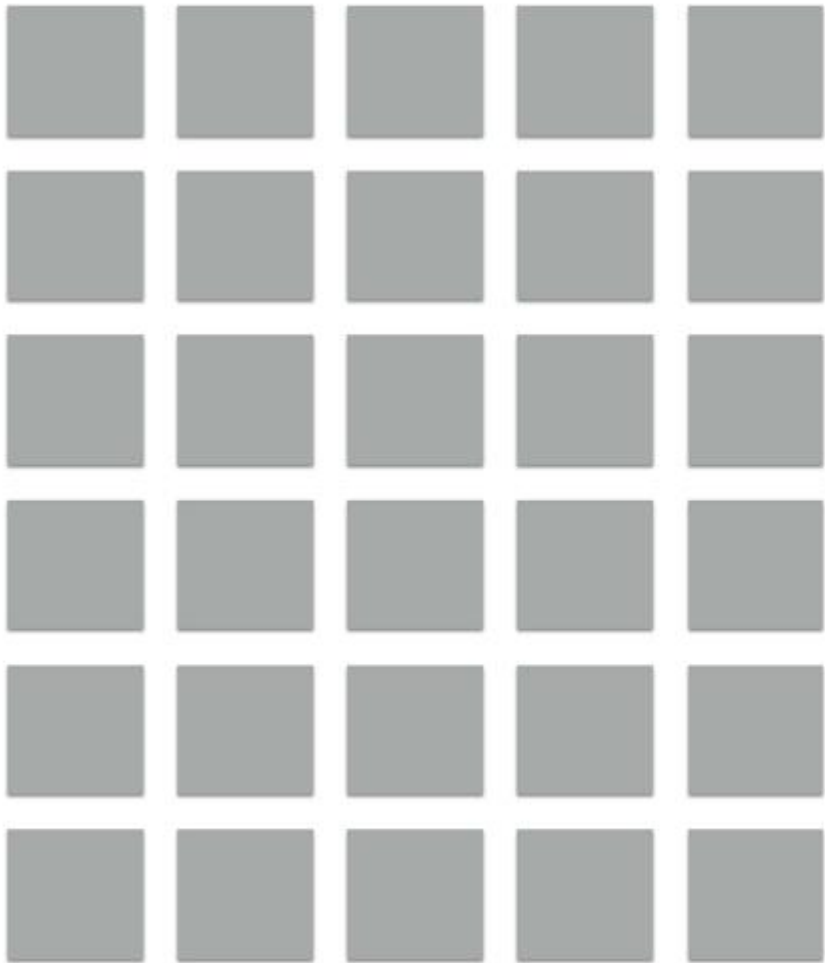
A new problem appears

Existing problems

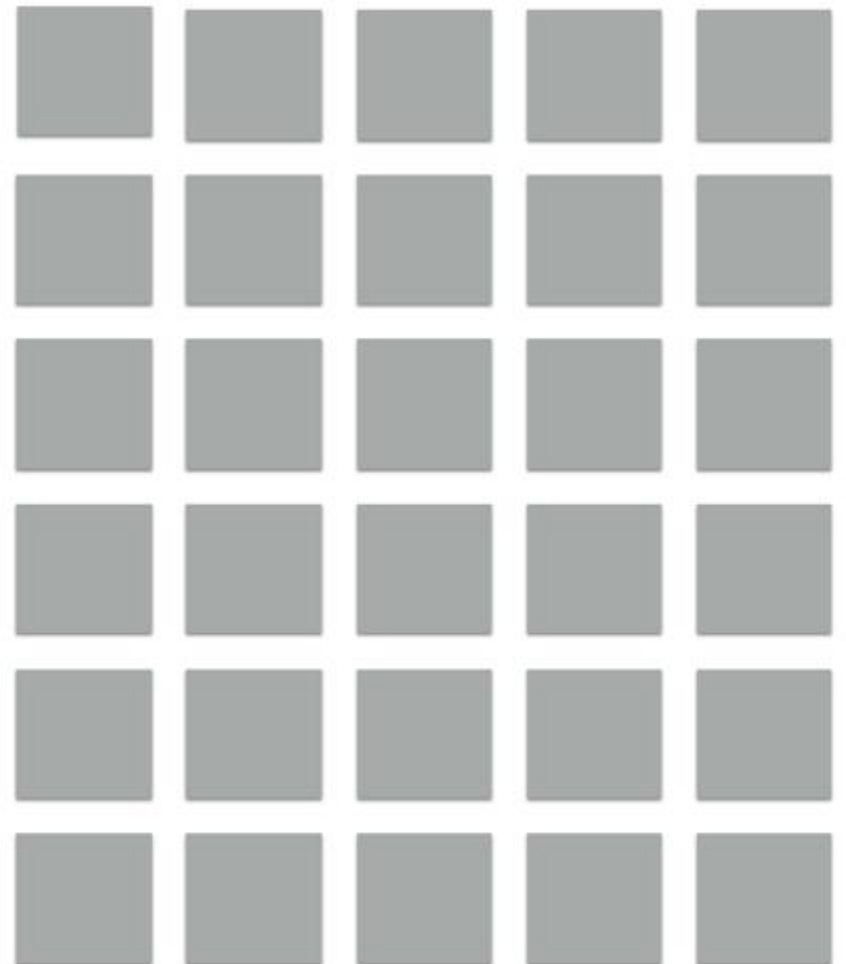


Event correlation

Existing problems

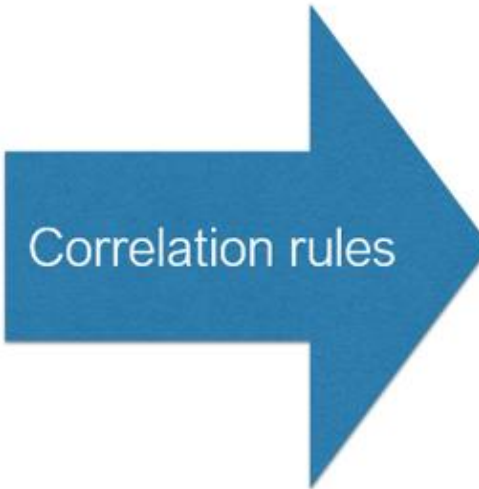
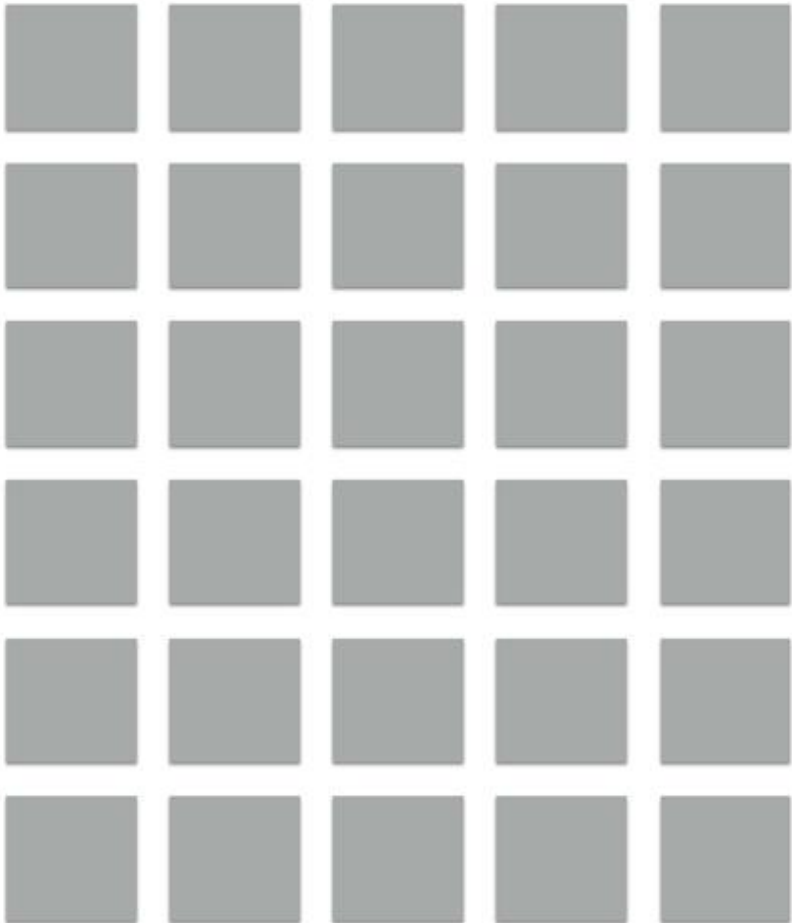


No correlation rules

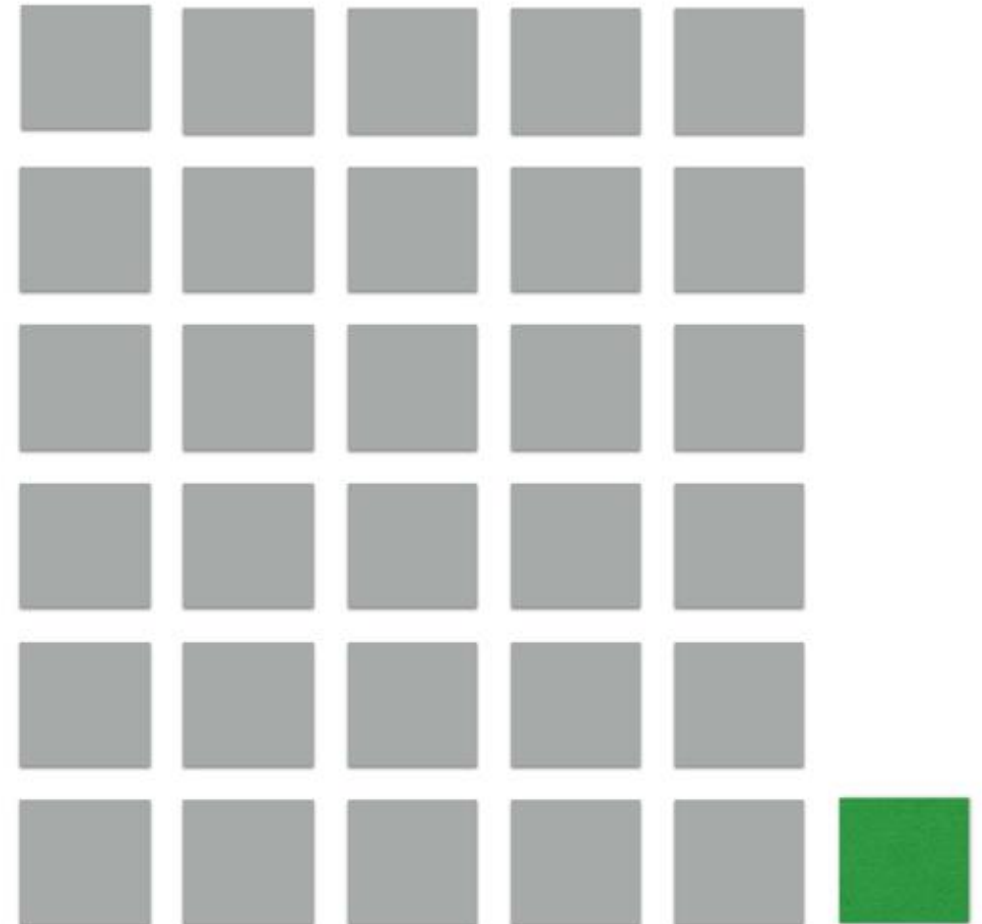


Event correlation

Existing problems

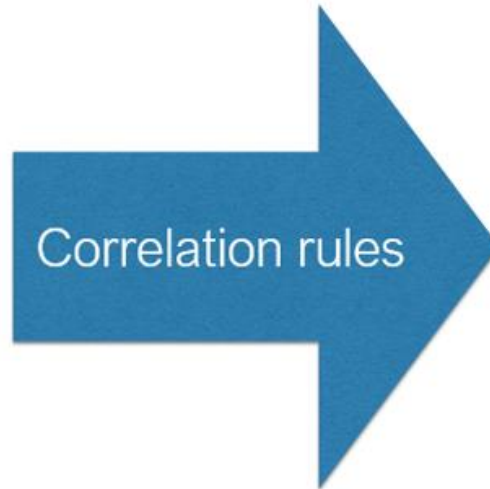
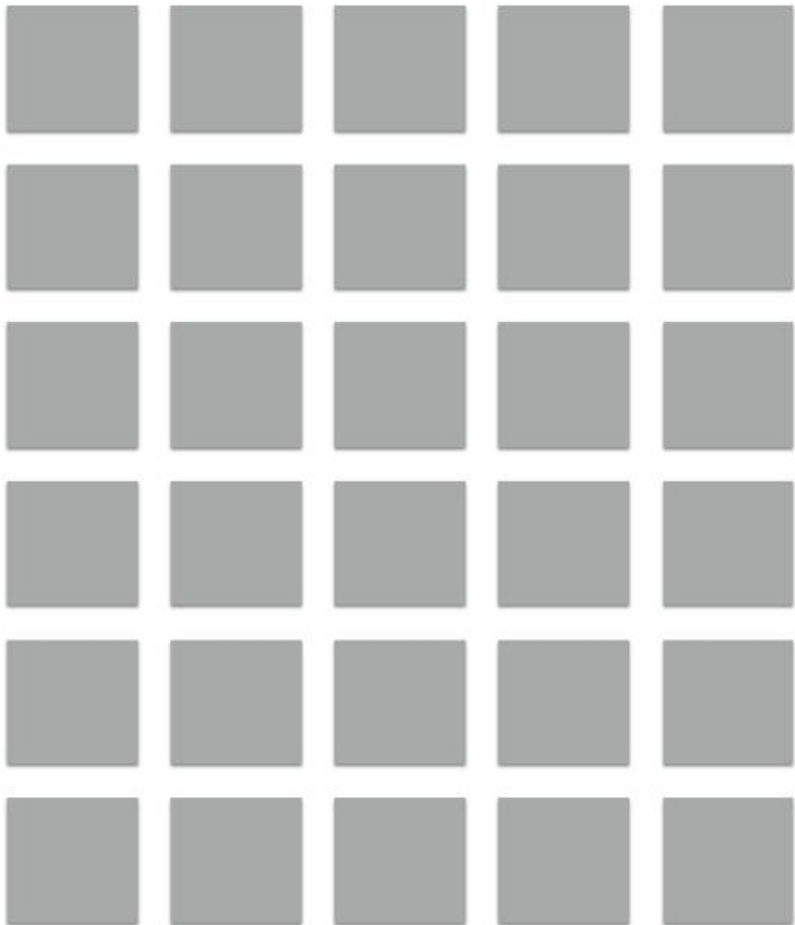


No correlation rules

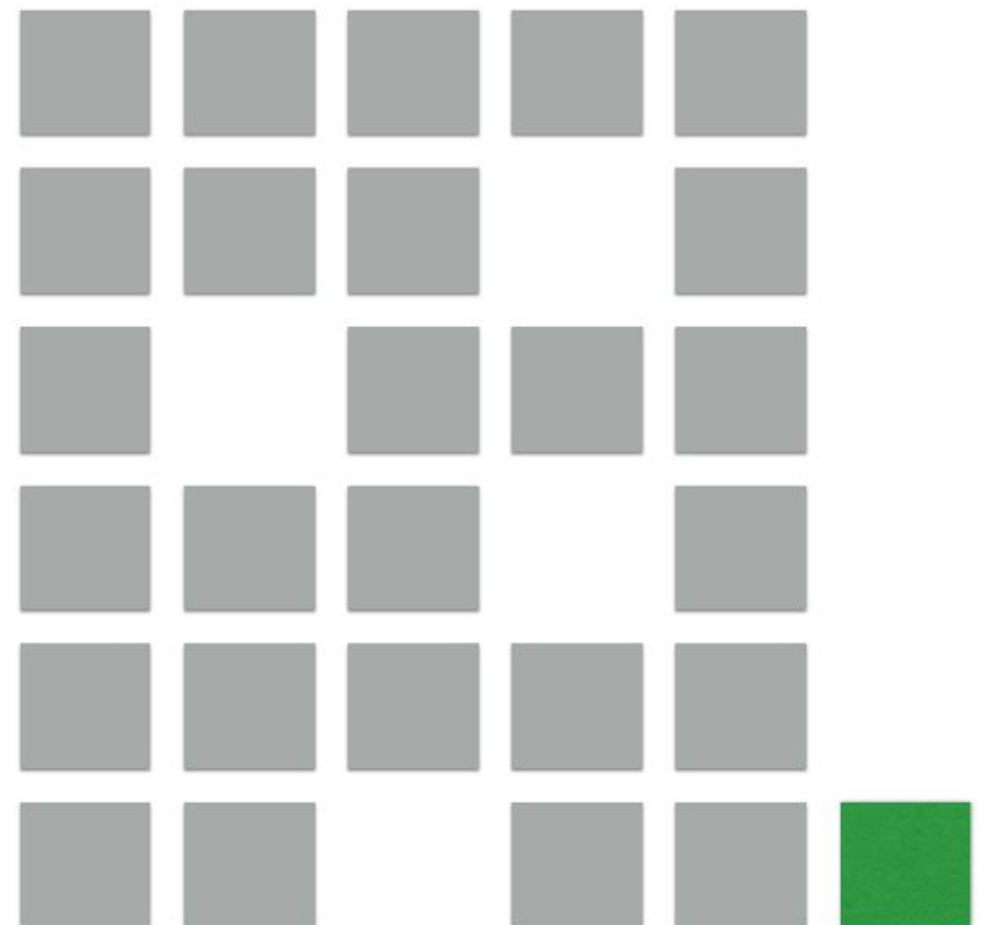


Event correlation

Existing problems



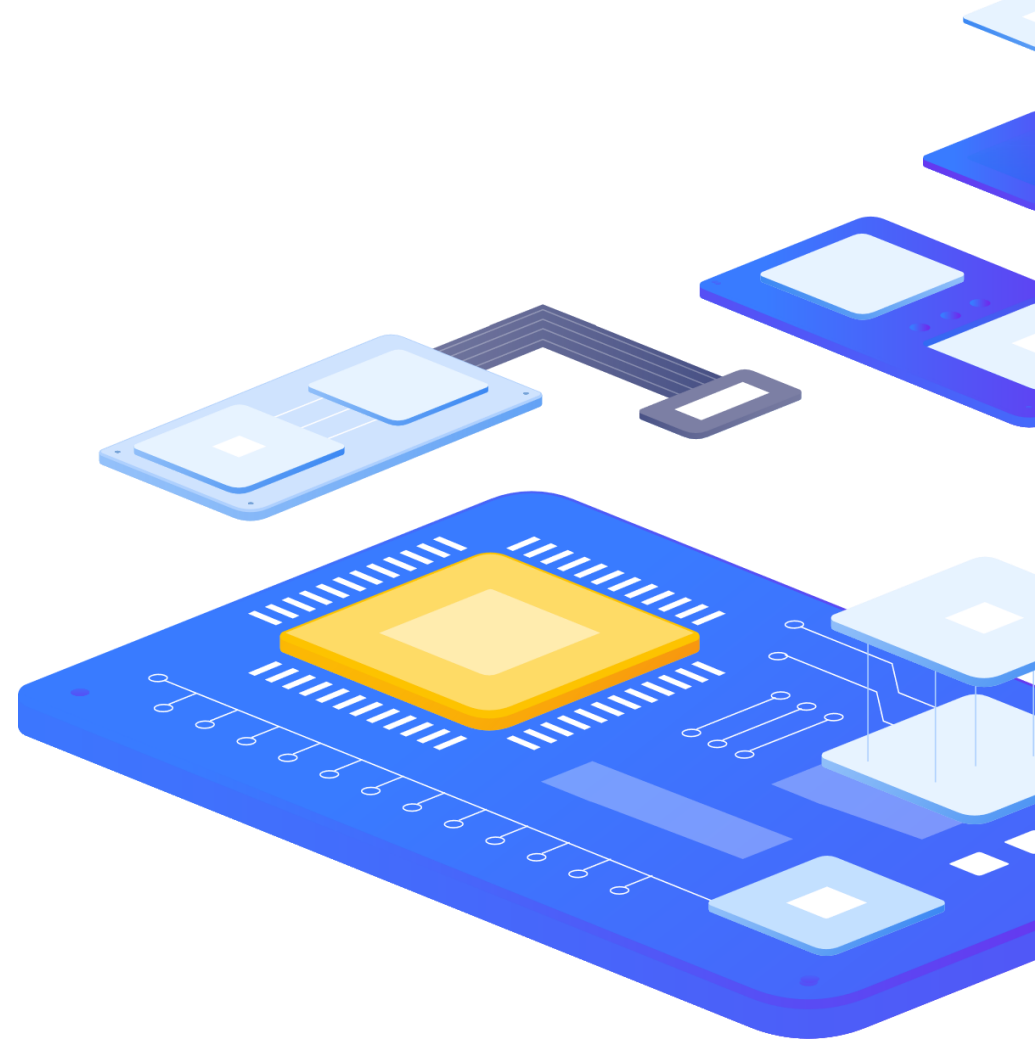
No correlation rules (close



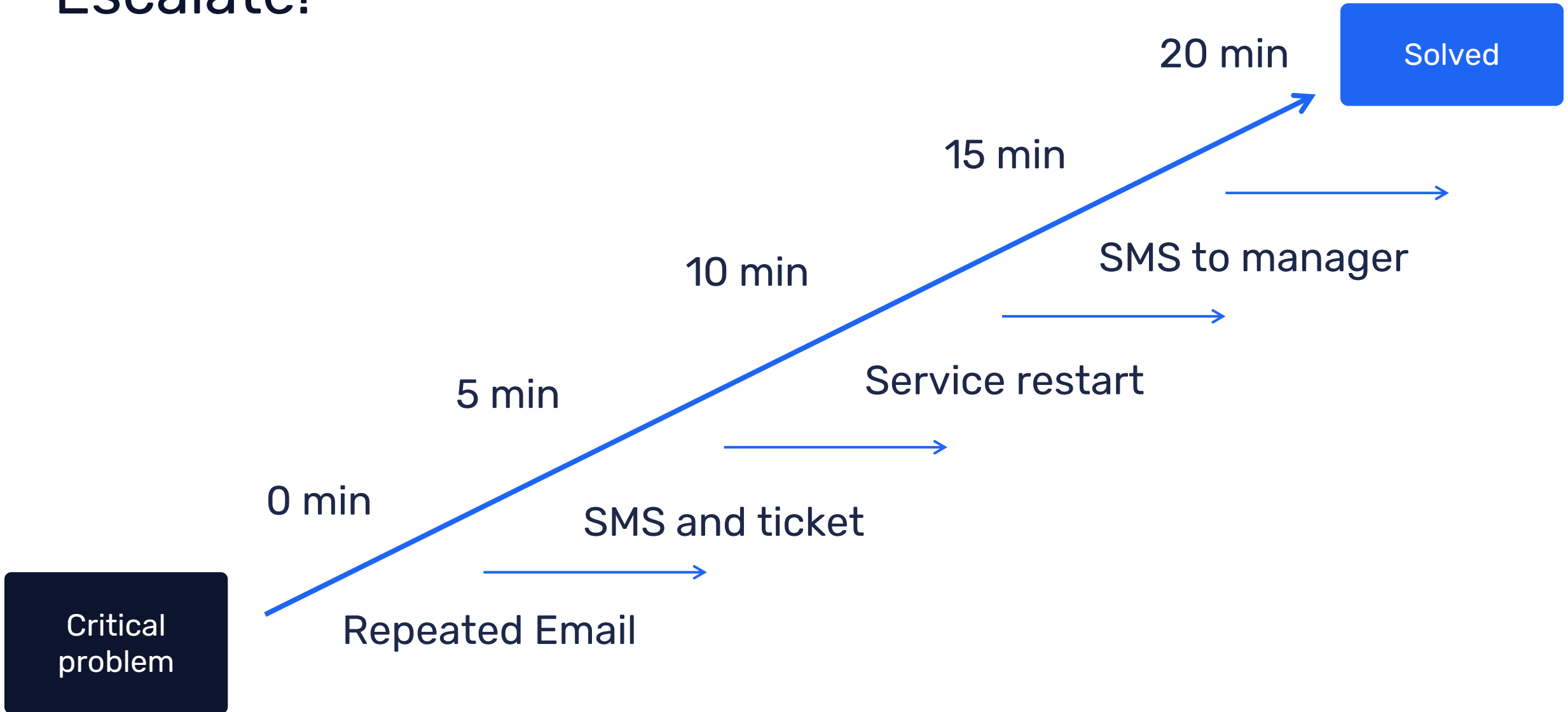
ADVANCED PROBLEM DETECTION

Escalate!

- › Immediate reaction
- › Delayed reaction
- › Notification if automatic action failed
- › Repeated notifications
- › Escalation to a new level



Escalate!



ADVANCED PROBLEM DETECTION

In summary

- › Analyze history
- › No problem!= Solution
- › Use different conditions for problem definition and recovery
- › Pay attention to anomaly detection
- › Use correlation
- › Resolve common problems automatically
- › Do not hesitate to escalate!



7

Expression macros

ADVANCED PROBLEM DETECTION

{?EXPRESSION_MACROS}

- ▶ If defined, this name will be used to create the problem event name, instead of the trigger name.
- ▶ The event name may be used to build meaningful alerts containing problem data
- ▶ The same set of macros is supported as in the trigger name, plus {TIME} and {?EXPRESSION} expression macros.
- ▶ Supported since Zabbix 5.2.0
- ▶ Can be used in different locations – **Event Name**, Maps, name of Graphs

ADVANCED PROBLEM DETECTION

{?EXPRESSION_MACROS}

Junior

- ▶ Problem: Load of **Exchange** server increased by more than 10% last month

Expert

- ▶ Problem: Load of **Exchange** server increased by **24%** in **July (0.69)** comparing to **June (0.56)**
- ▶ Load of {HOST.HOST} server increased by
 - ▶ `{{?100*trendavg(//system.cpu.load,1M:now/M)/trendavg(//system.cpu.load,1M:now/M-1M)}.fmtnum(0)}%` in
 - ▶ `{{TIME}.fmttime(%B,-1M)}`
 - ▶ `({{?trendavg(//system.cpu.load,1M:now/M)}.fmtnum(2)})` comparing to
 - ▶ `{{TIME}.fmttime(%B,-2M)}`
 - ▶ `({{?trendavg(//system.cpu.load,1M:now/M-1M)}.fmtnum(2)})`

<https://www.zabbix.com/documentation/6.0/en/manual/config/triggers/expression?hl=expression#examples-of-triggers>

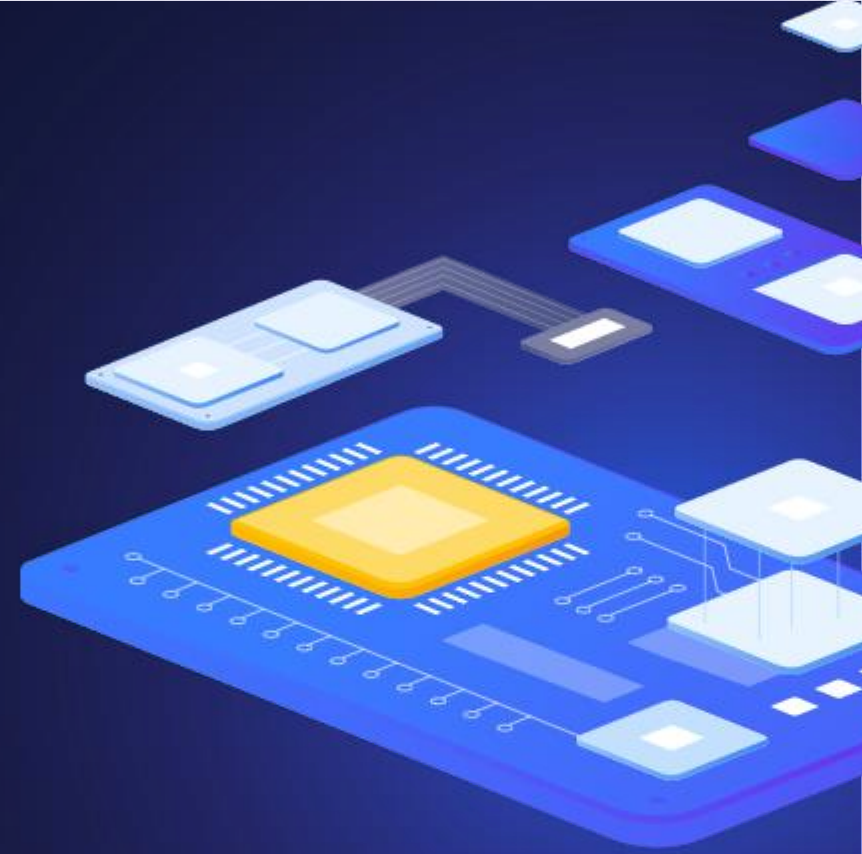
8

Demo



9

Questions



CONTACT US:

Phone:



+420 800 244 442

Web:



<https://www.initmax.cz>

Email:



tomas.hermanek@initmax.cz

LinkedIn:



<https://www.linkedin.com/company/initmax>

Twitter:



<https://twitter.com/initmax>

Tomáš Heřmánek:



+420 732 447 184