initMAX

Webinar

Advanced problem detection

all our microphones are muted

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

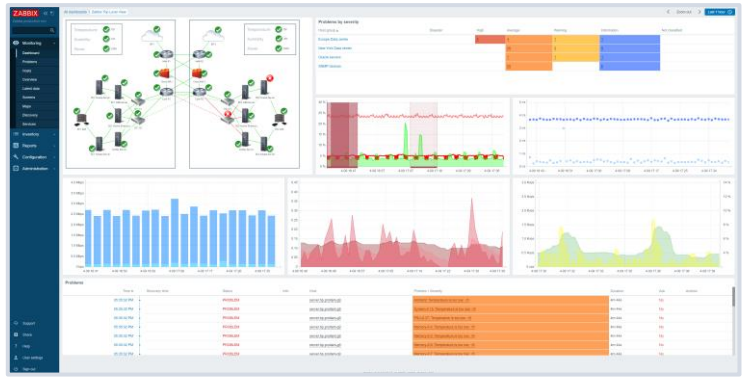
use Chat for discussion, networking or applause

1

Zabbix data flow

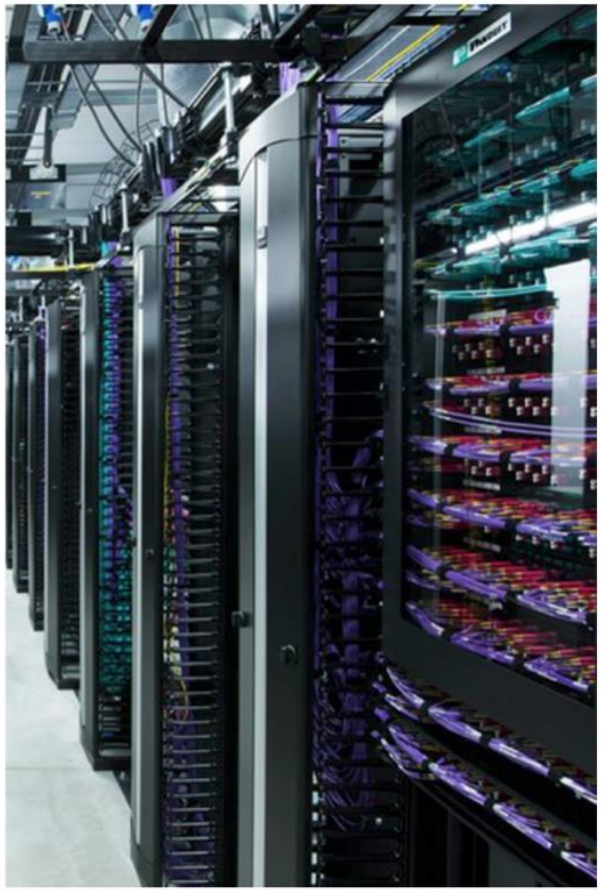
ADVANCED PROBLEM DETECTION

Zabbix data flow



Visualization

Notifications



DATABASE

ZABBIX SERVER

History

Analysis

Data collection

ADVANCED PROBLEM DETECTION

How often to execute checks?

Every N seconds

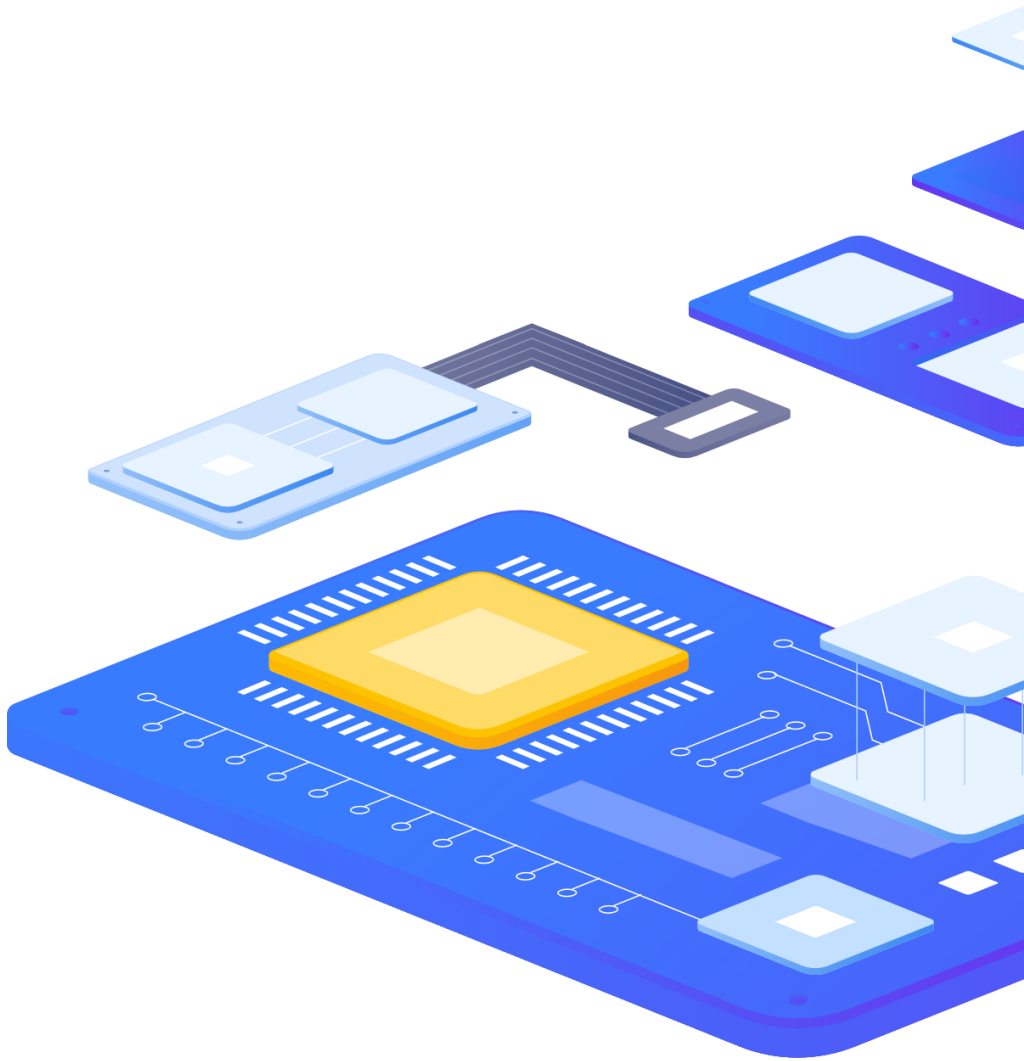
- Zabbix will evenly distribute checks

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

initMAX

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

initMAX

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

initMAX

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)

initMAX

ADVANCED PROBLEM DETECTION

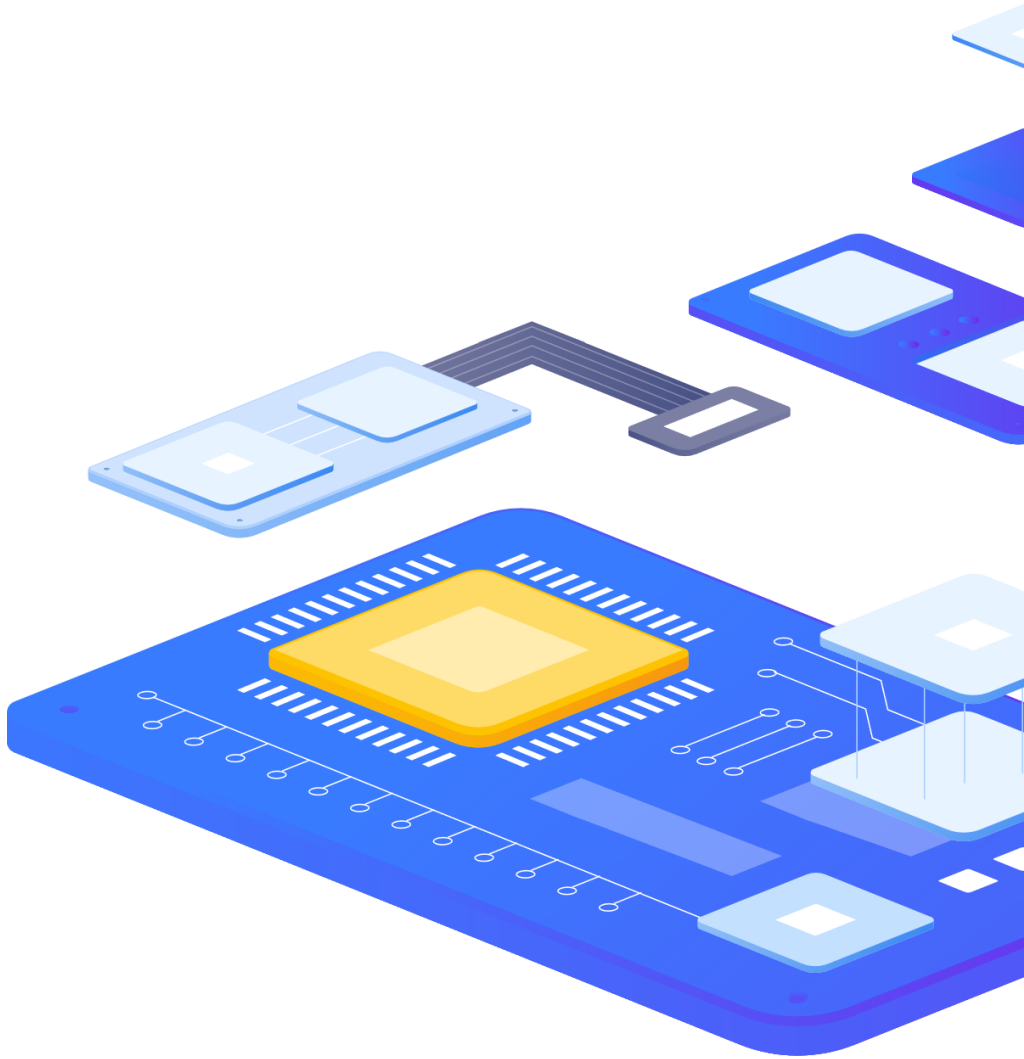
Junior level

Performance

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

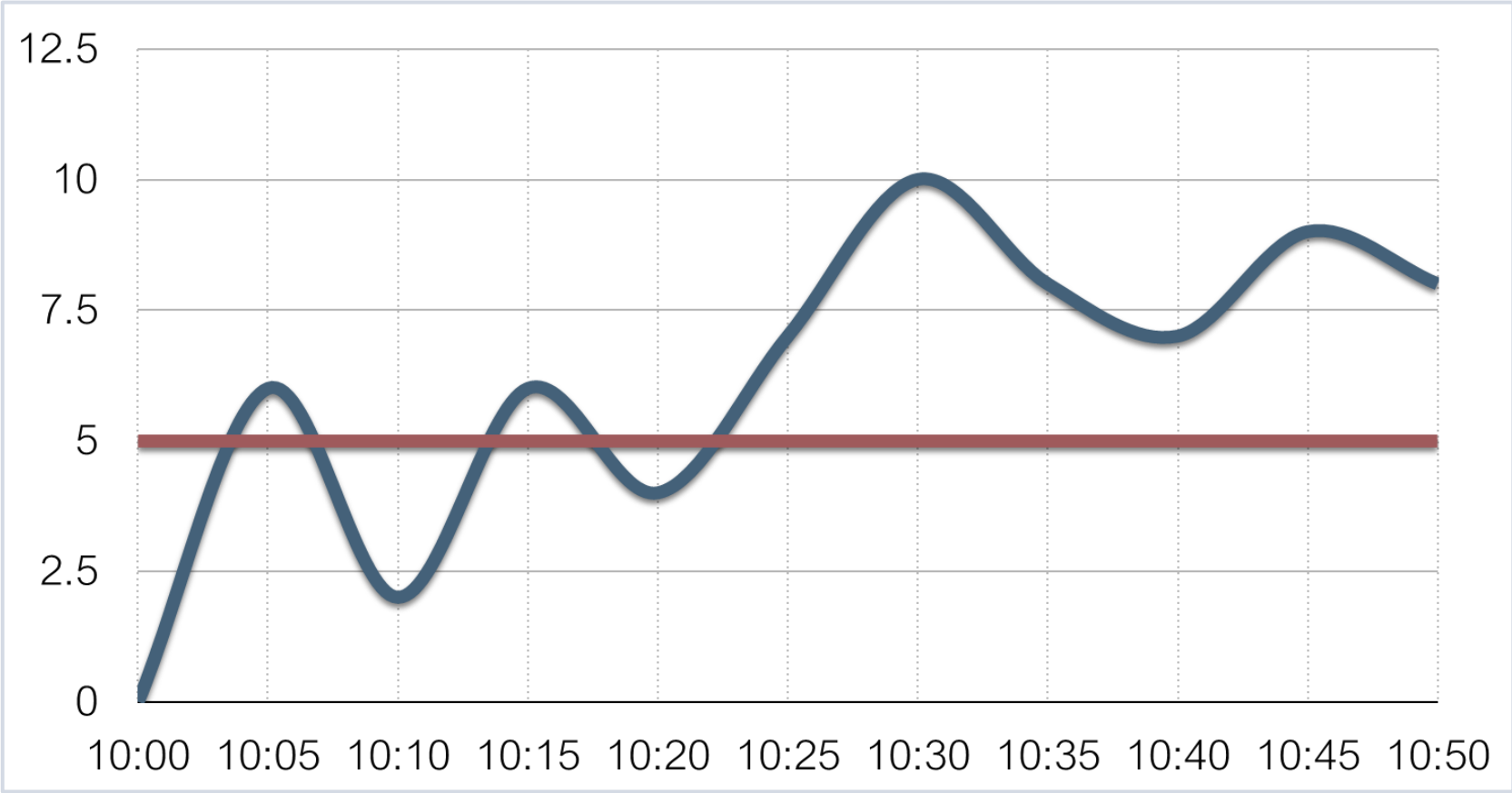
Availability

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



initMAX

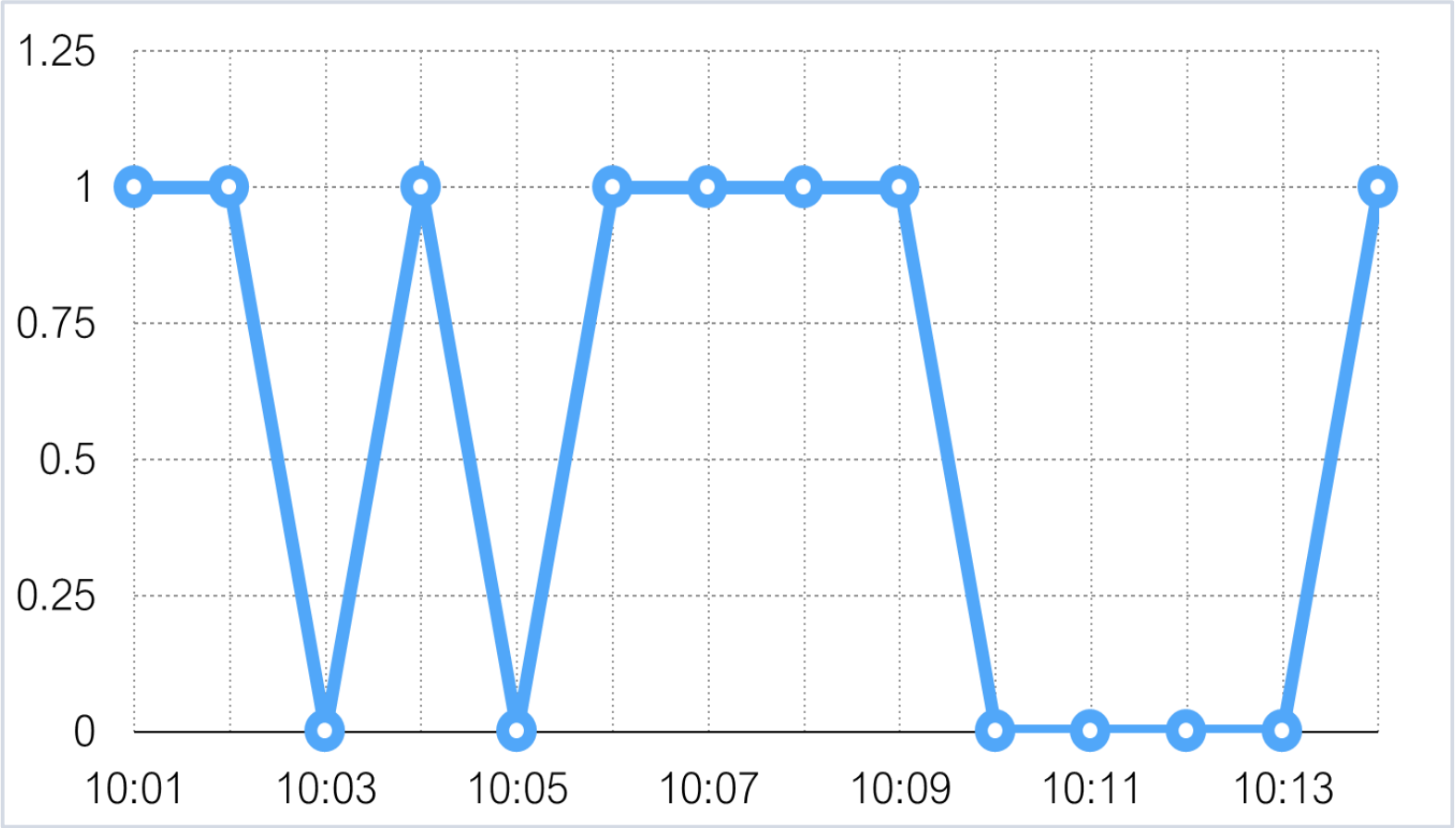
False positives



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

ADVANCED PROBLEM DETECTION

Too sensitive



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

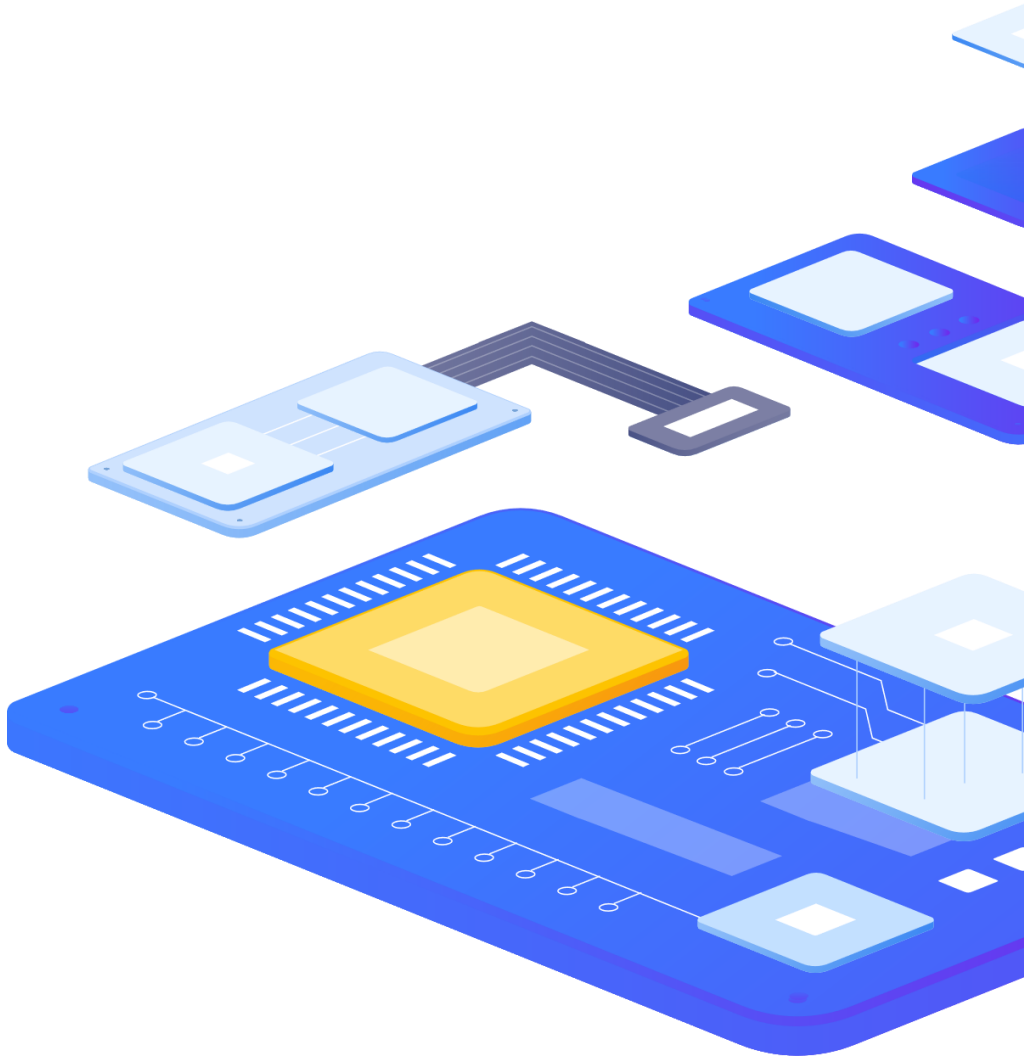
initMAX

ADVANCED PROBLEM DETECTION

Junior level

Too sensitive leads to

- False positives



3

False positives

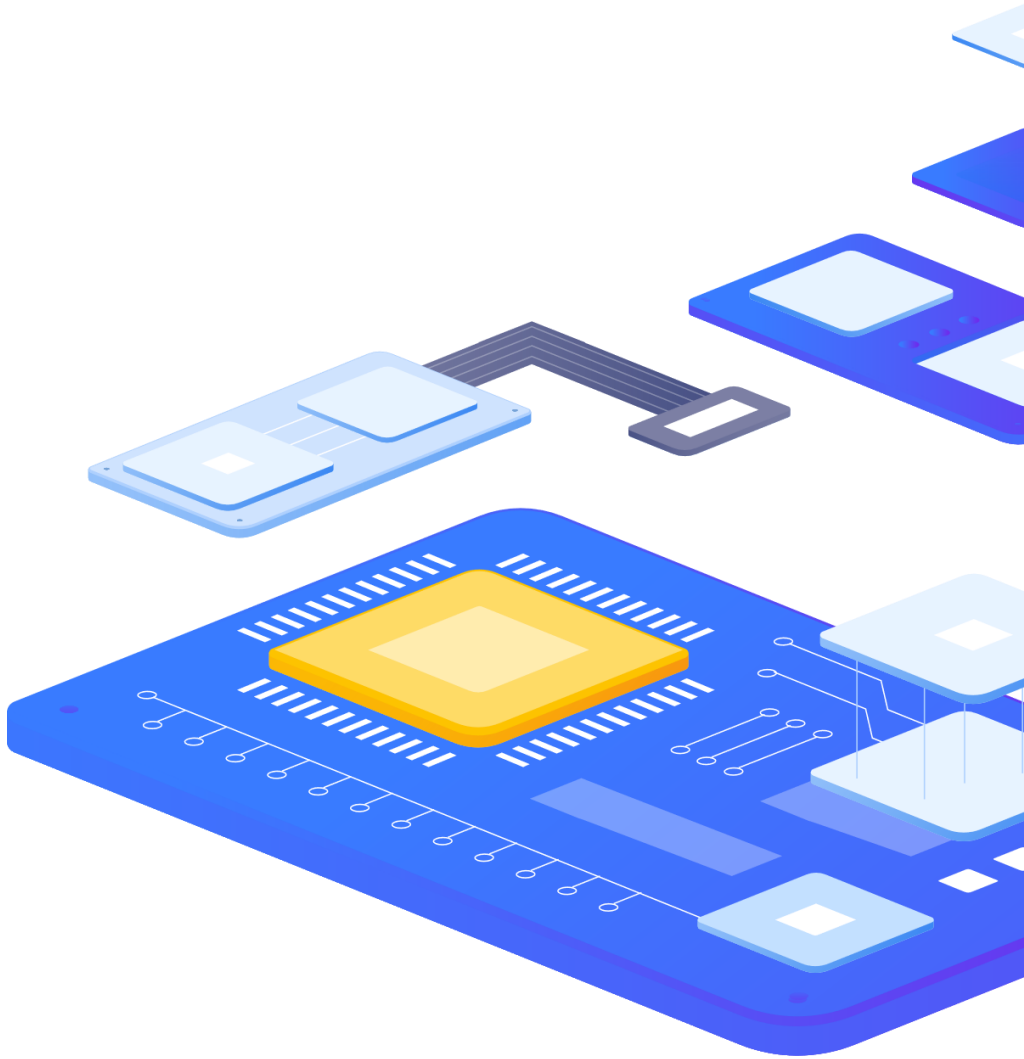
initMAX

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



initMAX

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?**

ADVANCED PROBLEM DETECTION

Analyze history

initMAX

Performance

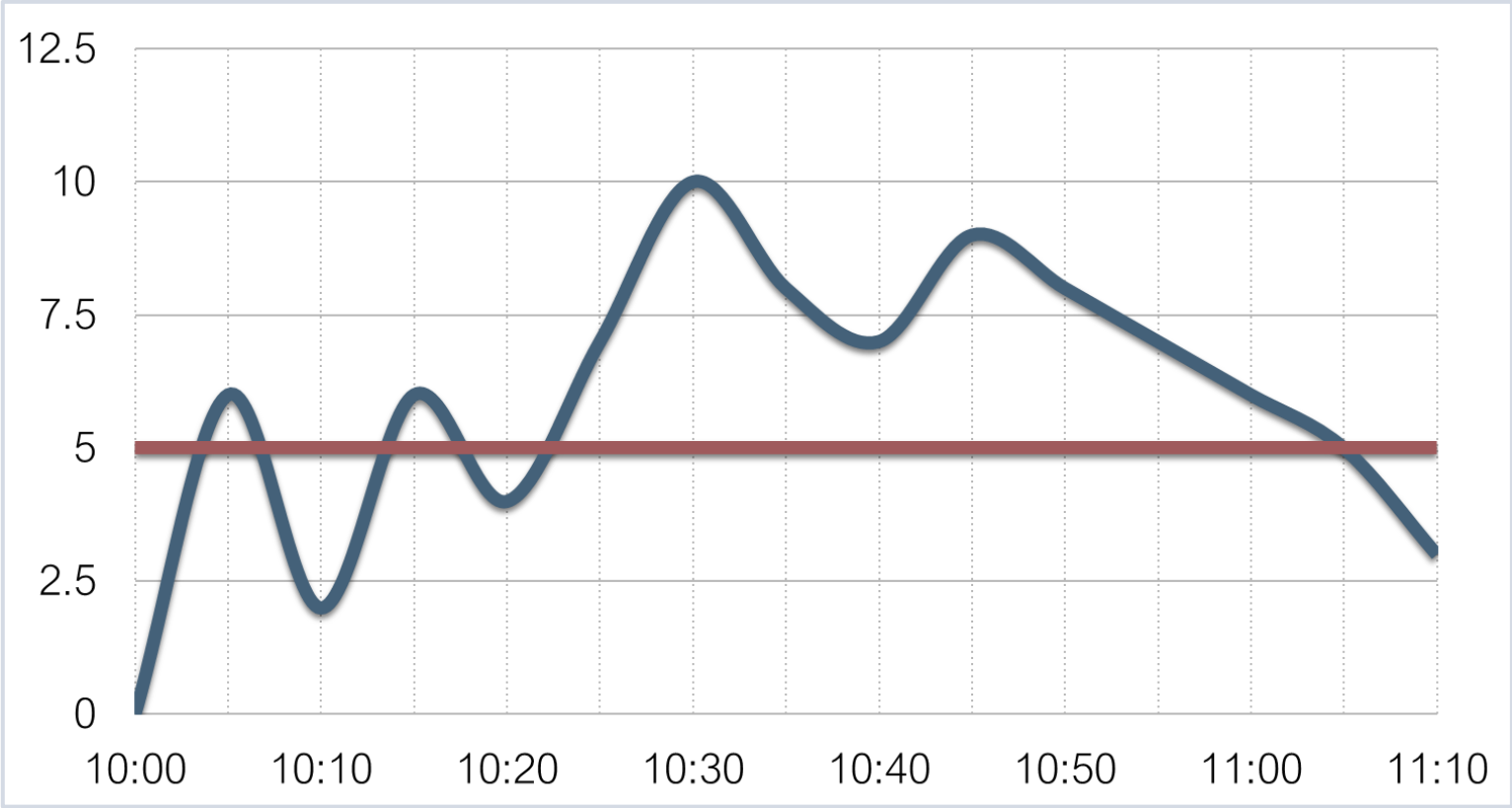
- min(/server/system.cpu.load,10m) > 5

Availability

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

ADVANCED PROBLEM DETECTION

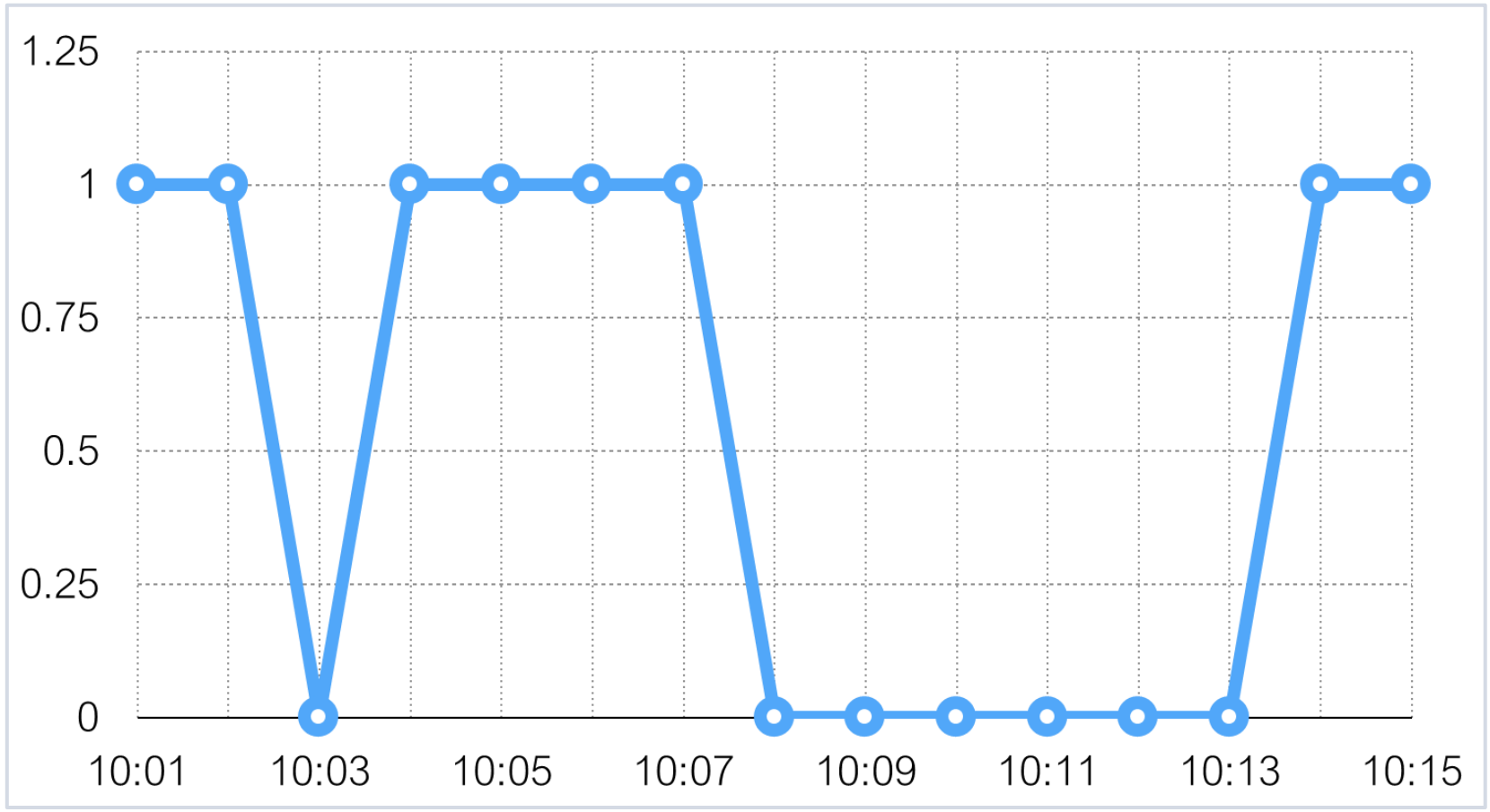
Analyze history



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

initMAX

Analyze history



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

initMAX

Different conditions for problem and recovery

Before

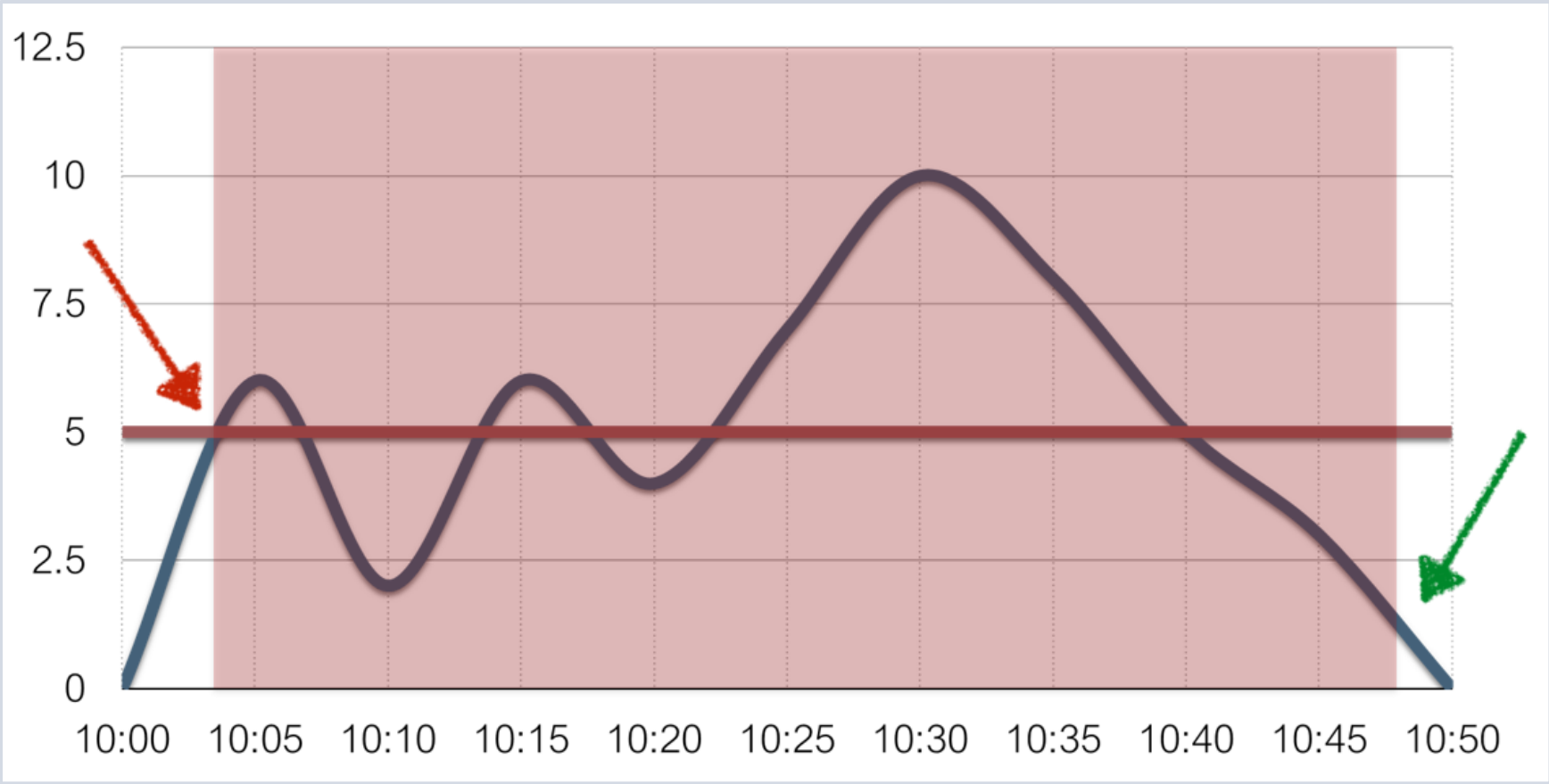
- last(/server/system.cpu.load) > 5

Now

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

initMAX

Different conditions for problem and recovery



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

initMAX

Examples

System is overloaded

Problem definition:

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

Recovery expression:

- max(/server/system.cpu.load,2m)<=1

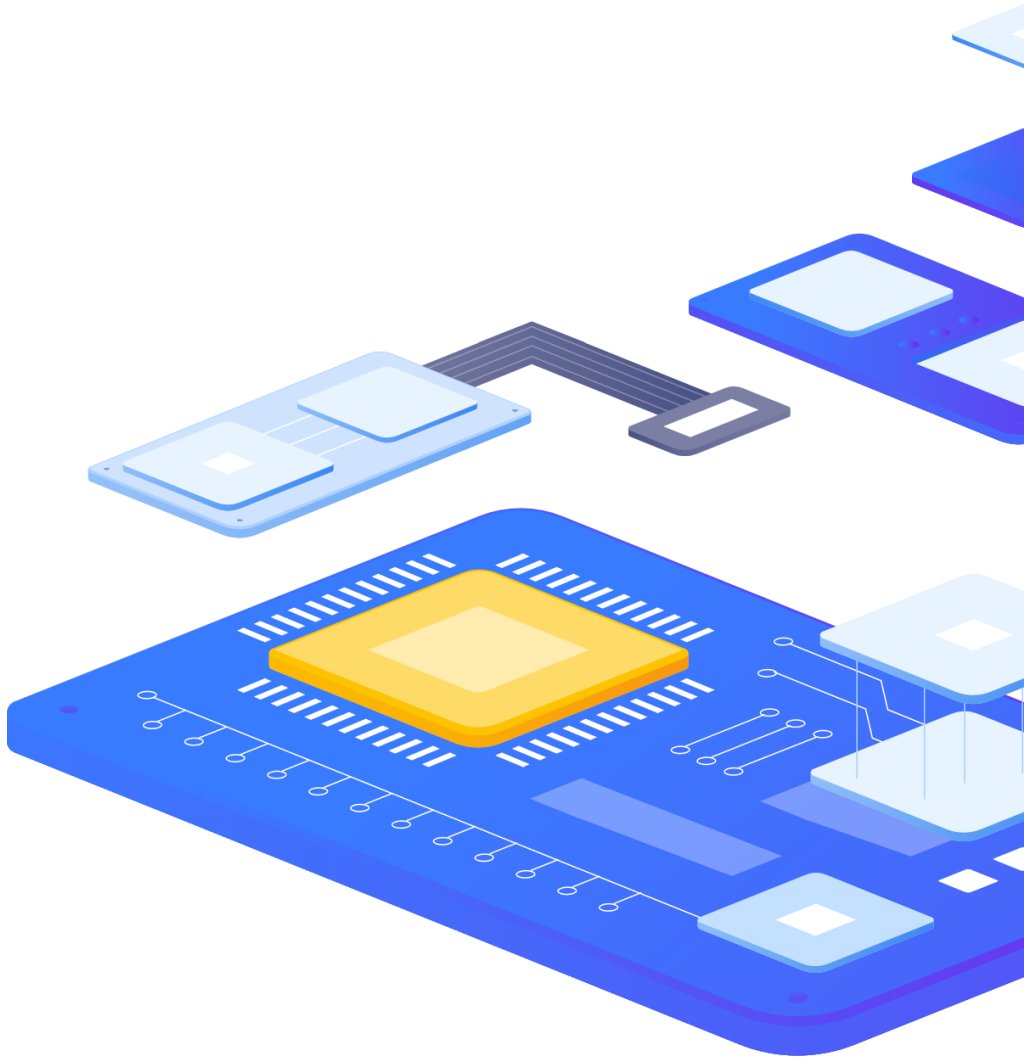
No free disk space /

Problem definition:

- last(/server/vfs.fs.size[/,pfree])<10

Recovery expression:

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



Examples

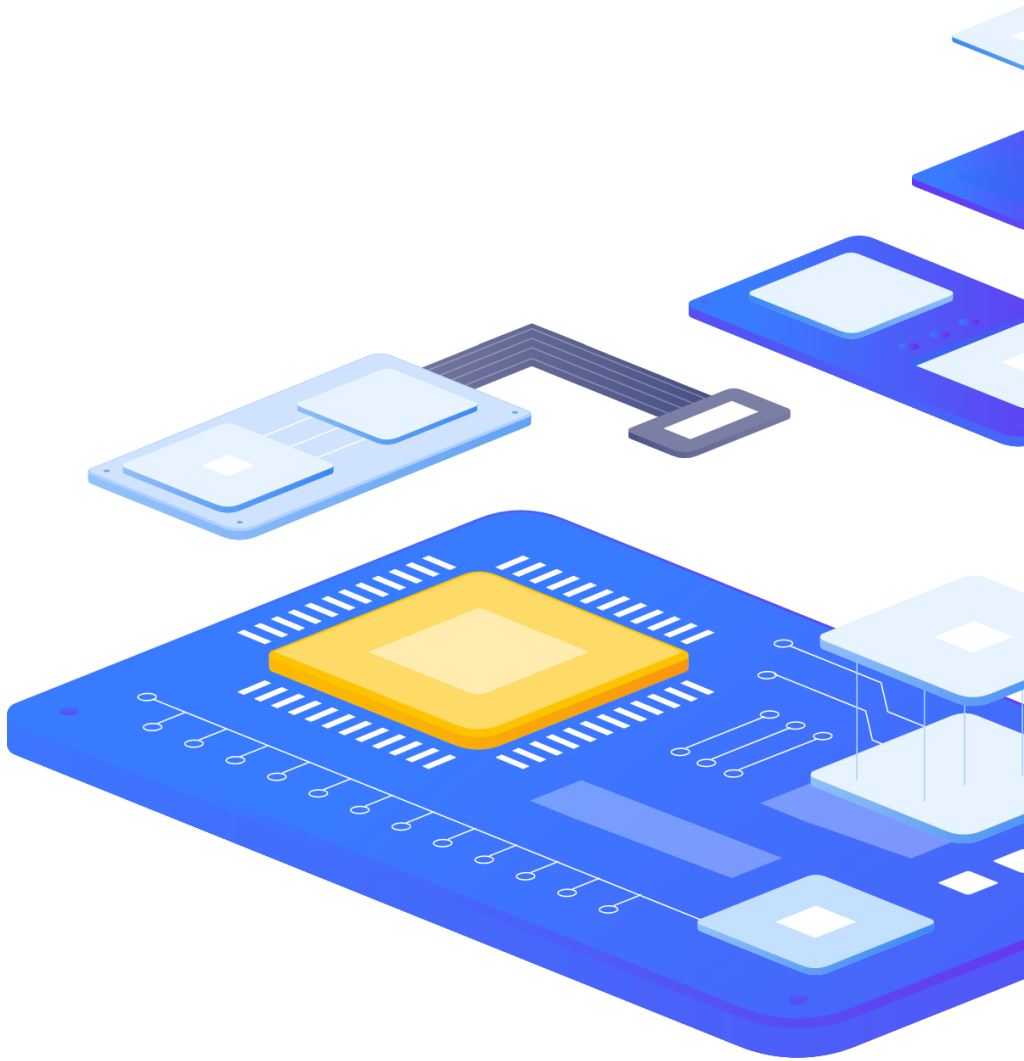
SSH is not available

Problem definition:

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

Recovery expression:

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



ADVANCED PROBLEM DETECTION

initMAX

Anomalies

How to detect?

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

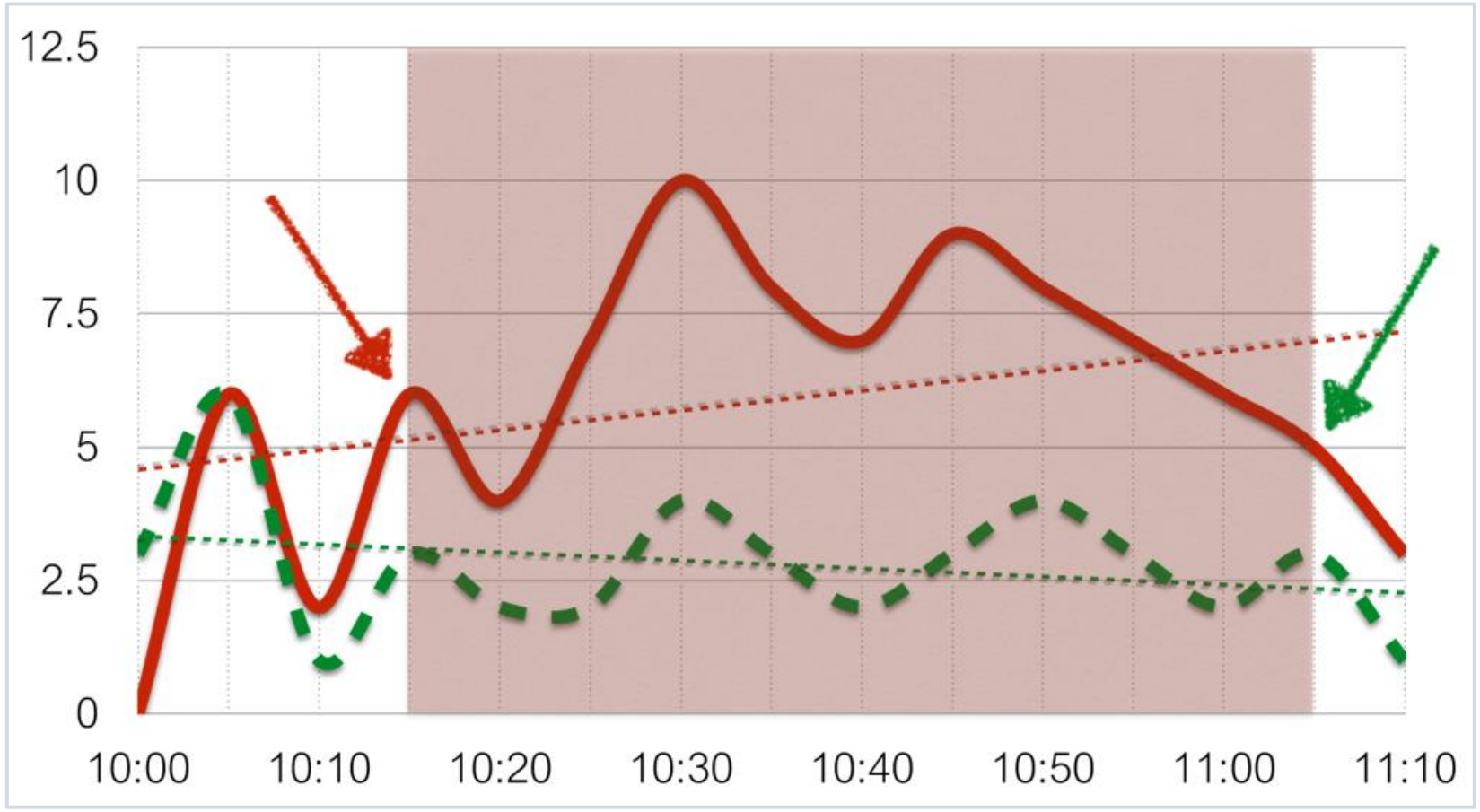
Average CPU load for the last hour is 2x higher than

CPU load for the same period week ago

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

ADVANCED PROBLEM DETECTION

Anomalies



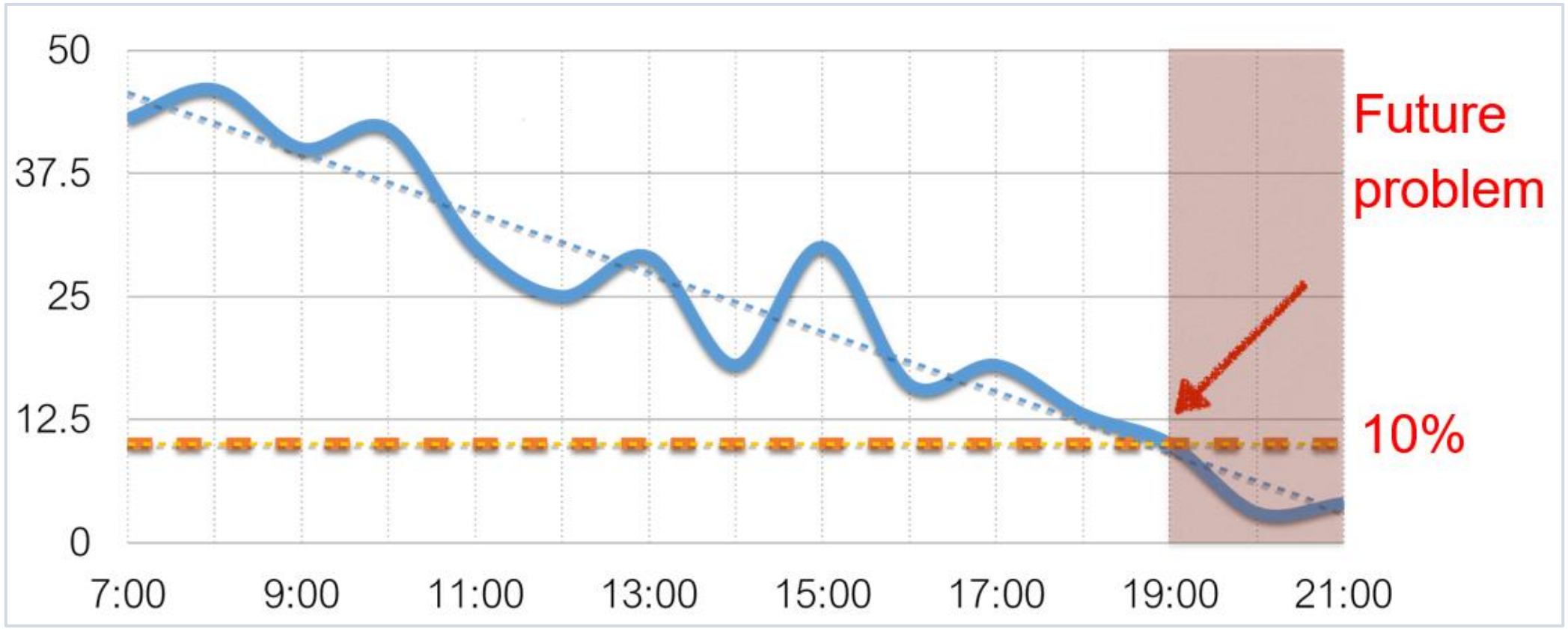
Comparison with the data 7 days ago

3

Forecast

initMAX

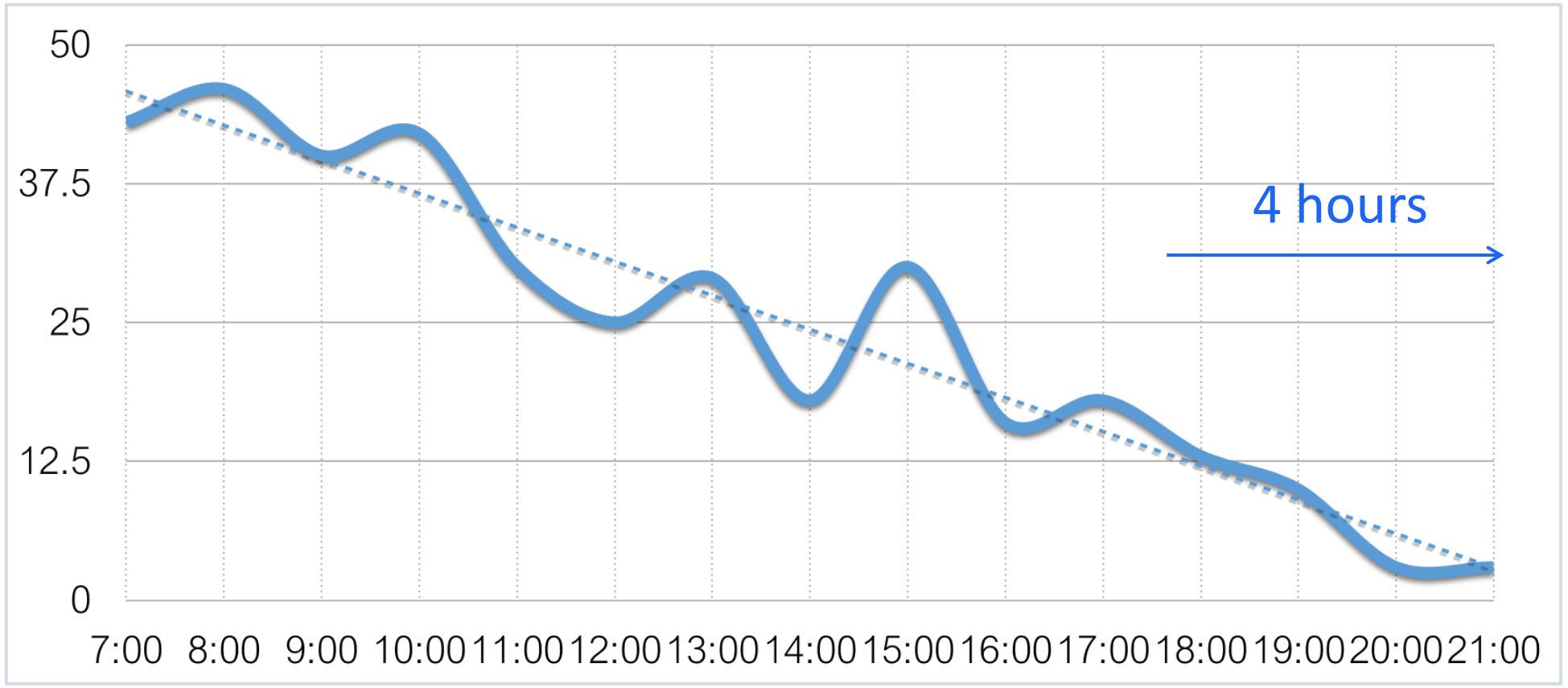
Forecast



Trigger function timeleft

ADVANCED PROBLEM DETECTION

Forecast



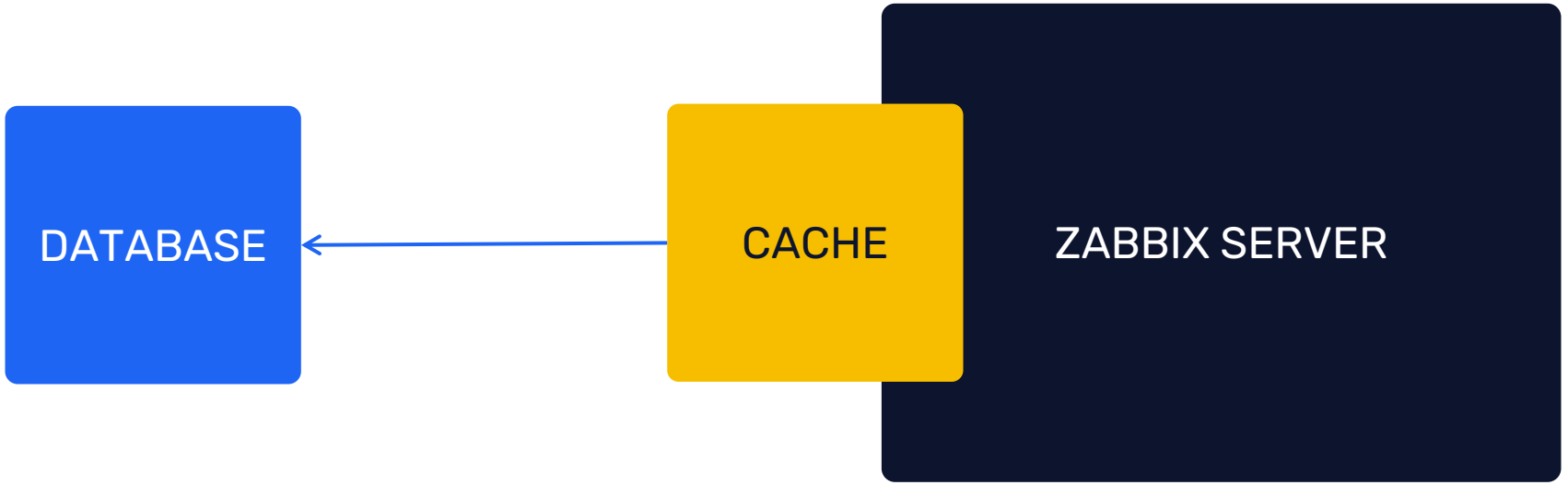
Trigger function forecast

initMAX

Does history analysis affect performance of Zabbix?

Yes, but not significantly.

Especially as of Zabbix 2.2.0.



4

Dependencies

initMAX

ADVANCED PROBLEM DETECTION

Dependencies

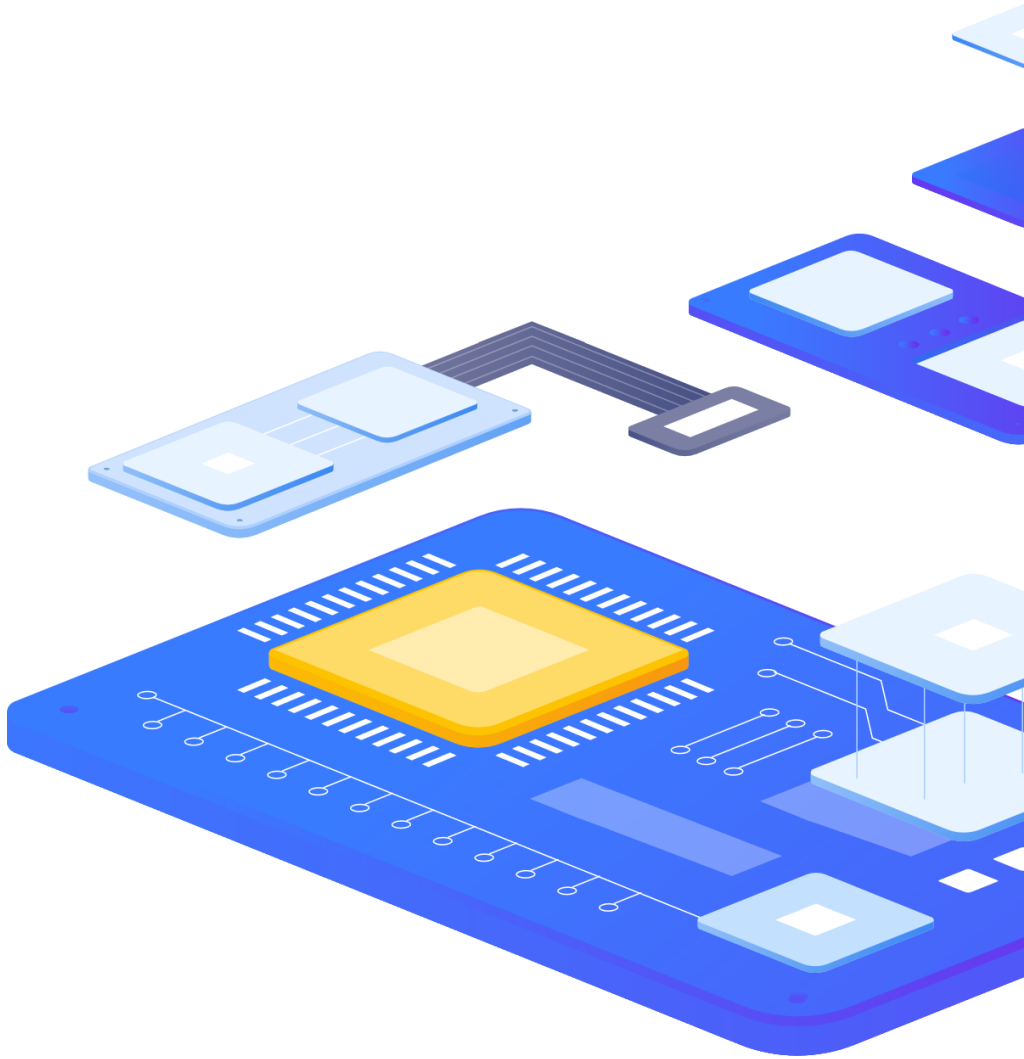
CRM is not working

↓

DB is unavailable

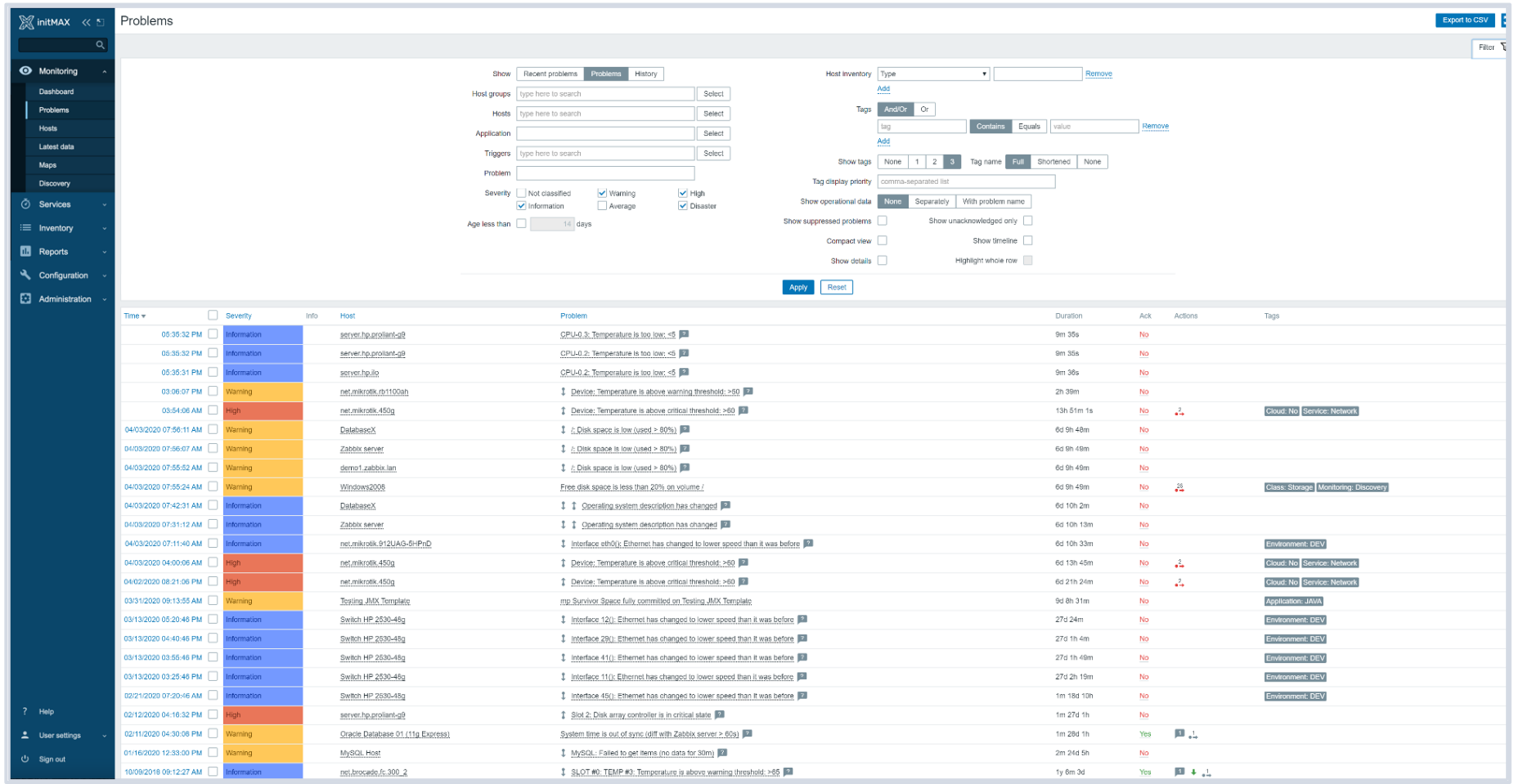
↓

No free diskspace



ADVANCED PROBLEM DETECTION

Section „Problems“



5

Tags

initMAX

Tags

Tag word: meaning

Customer: Alza
Customer: Globus

Datacenter: NY2
Datacenter: San Francisco

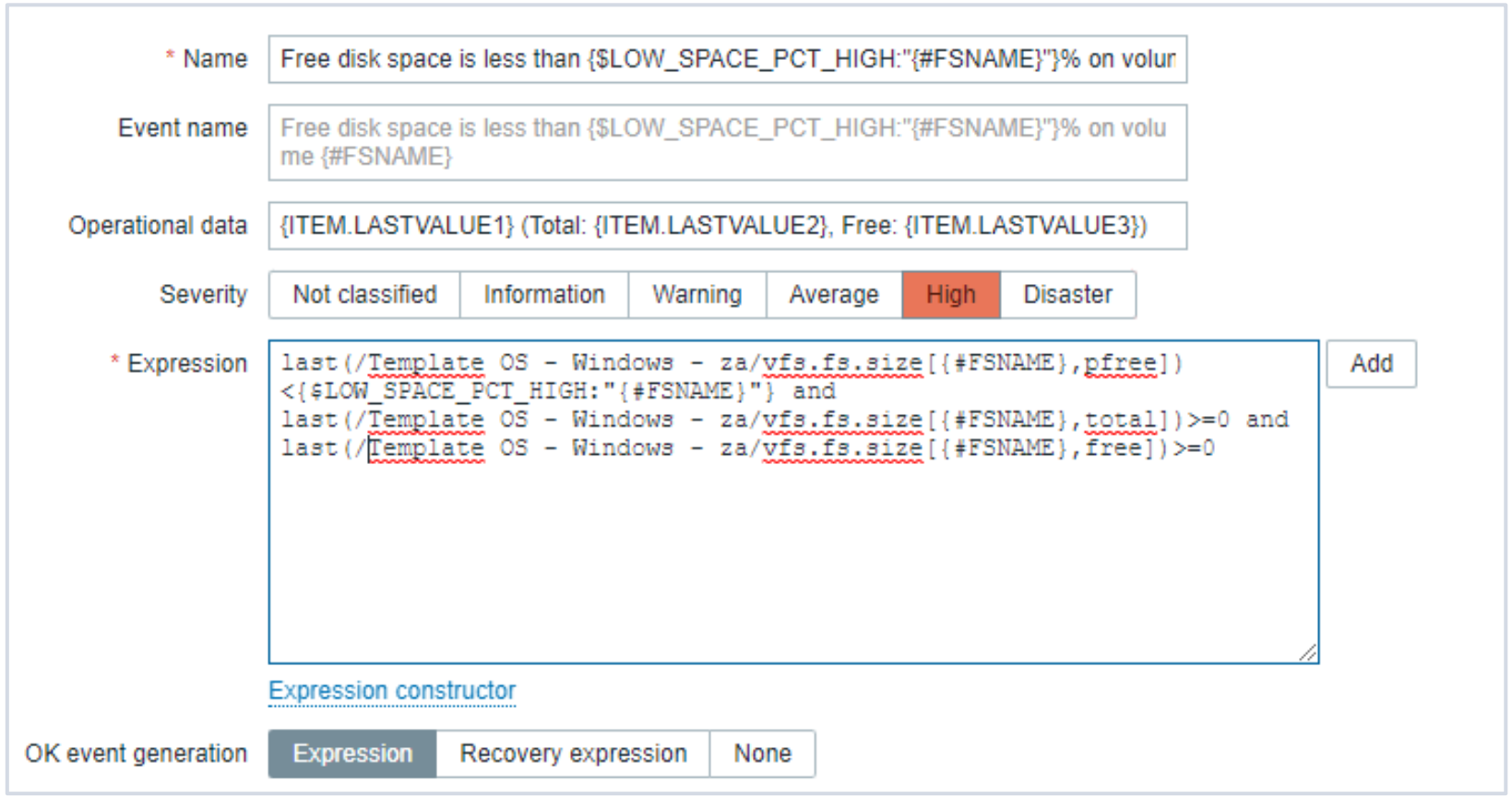
Area: Performance
Area: Availability
Area: Security

Environment: Staging
Environment: Test

User impact: None
User impact: Critical

Use of obtained values

Use of useful information in tags or names



ADVANCED PROBLEM DETECTION

Possible reactions

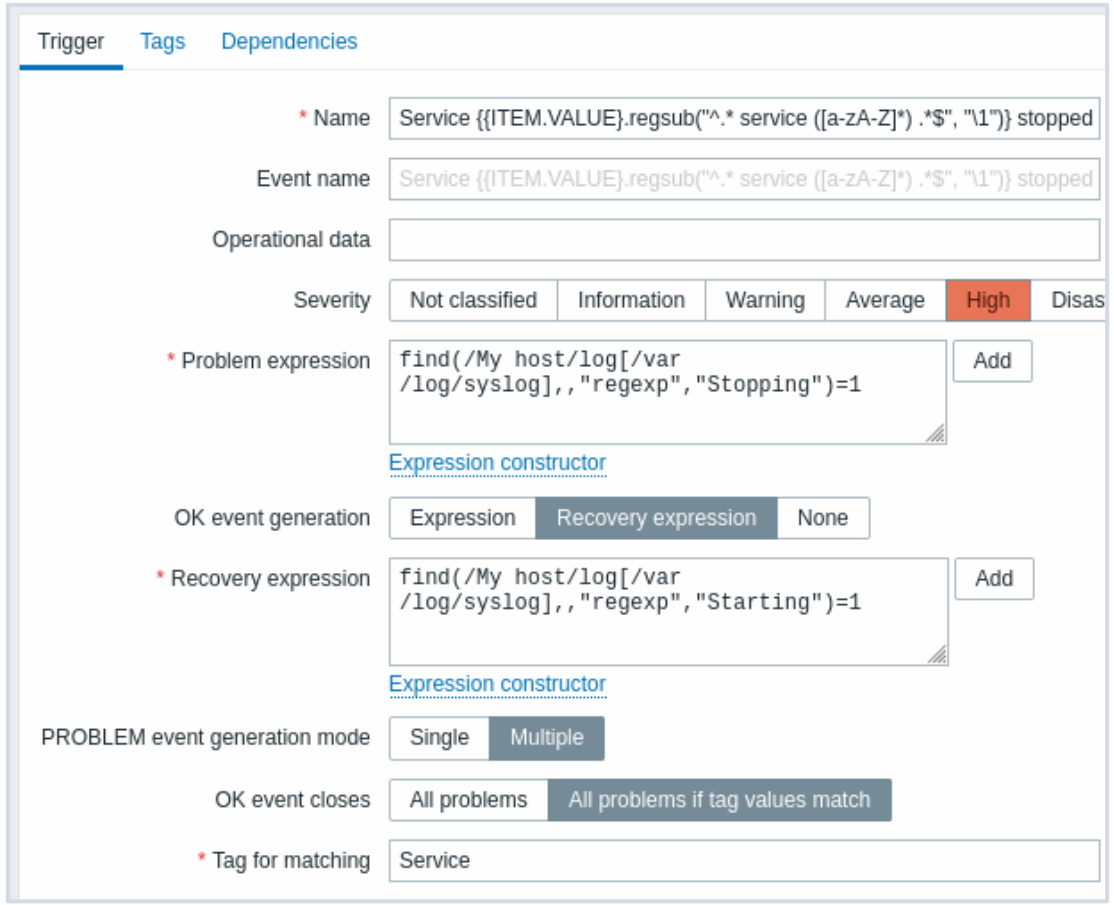
- Event correlation
- Automatized problem solving
- Manual problem closing
- Sending notifications to a user or a group of users
- Registration of tasks in the Helpdesk system

6

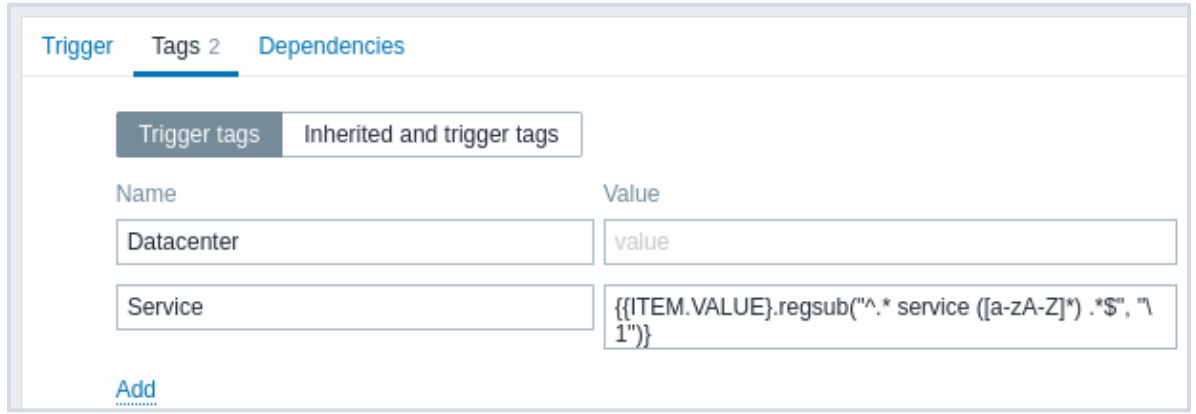
Event correlations

initMAX

Event correlation on trigger level



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



ADVANCED PROBLEM DETECTION

Event correlation on trigger level

initMAX

How does it work?

10/Feb/2022:06:25:30 service Jira stopped	“Service Jira 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”	PROBLEM

ADVANCED PROBLEM DETECTION

Event correlation on trigger level

initMAX

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

initMAX

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

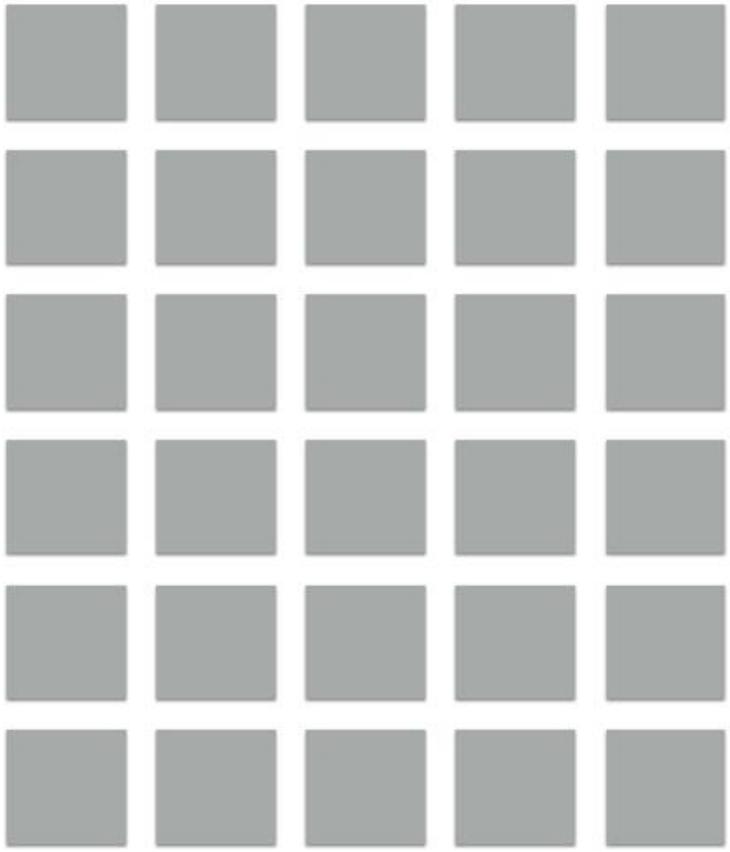
How does it work?

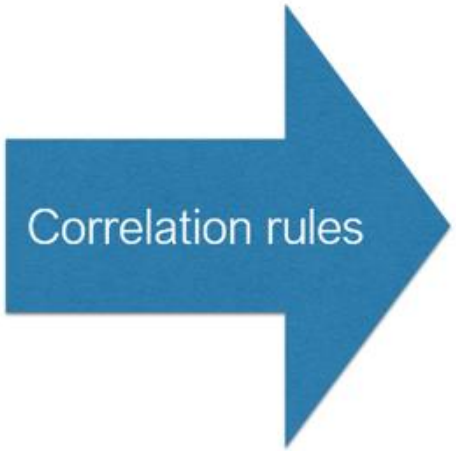
10/Feb/2022:06:25:30 service Jira stopped	“Service Jira stopped”	RESOLVED
10/Feb/2022:06:27:32 service MySQL stopped	“Service MySQL stopped”	RESOLVED
10/Feb/2022:06:28:11 service MySQL started		
10/Feb/2022:06:34:22 service Redis stopped	“Service Redis stopped”	RESOLVED
10/Feb/2022:06:37:58 service Redis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

Event correlation

A new problem appears

Existing problems

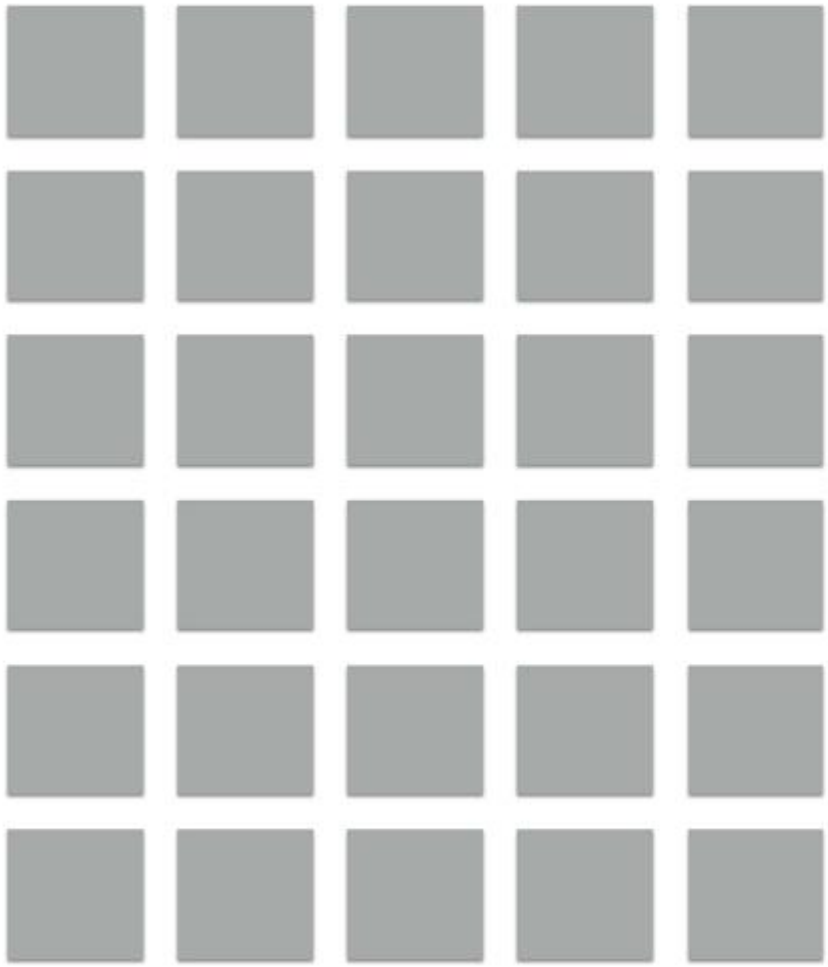


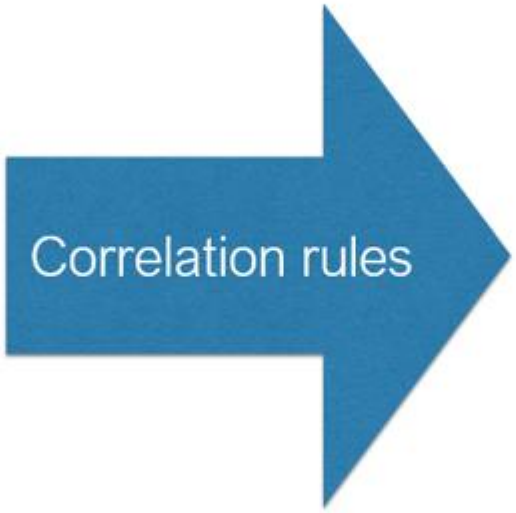


initMAX

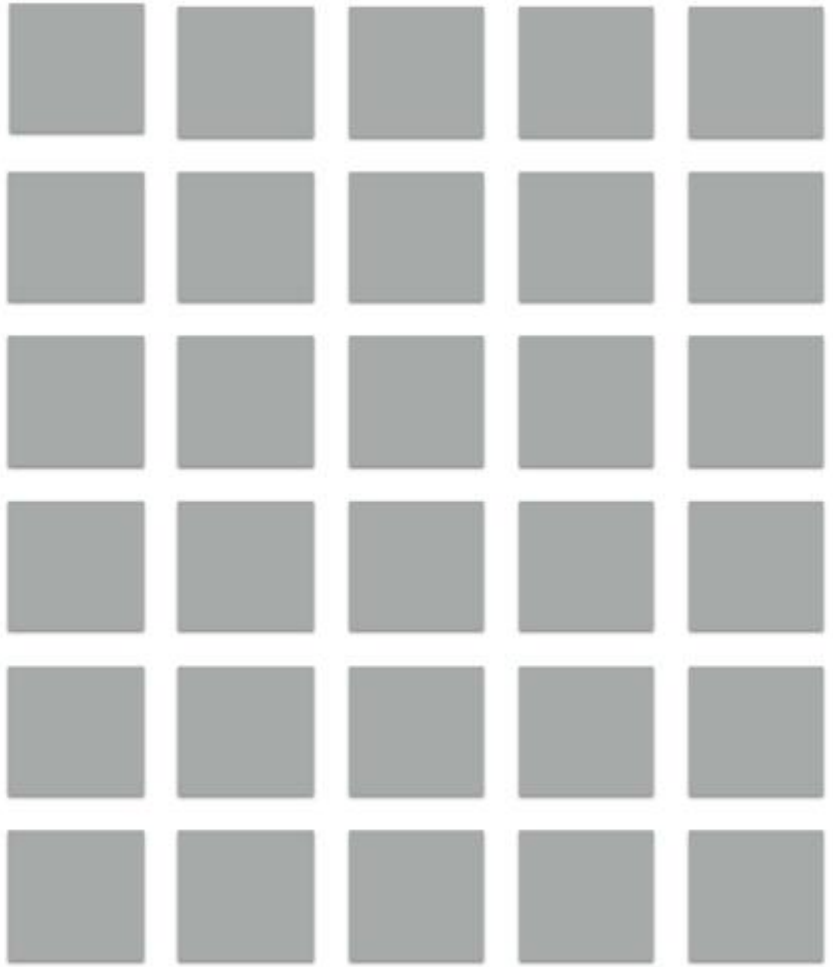
Event correlation

Existing problems





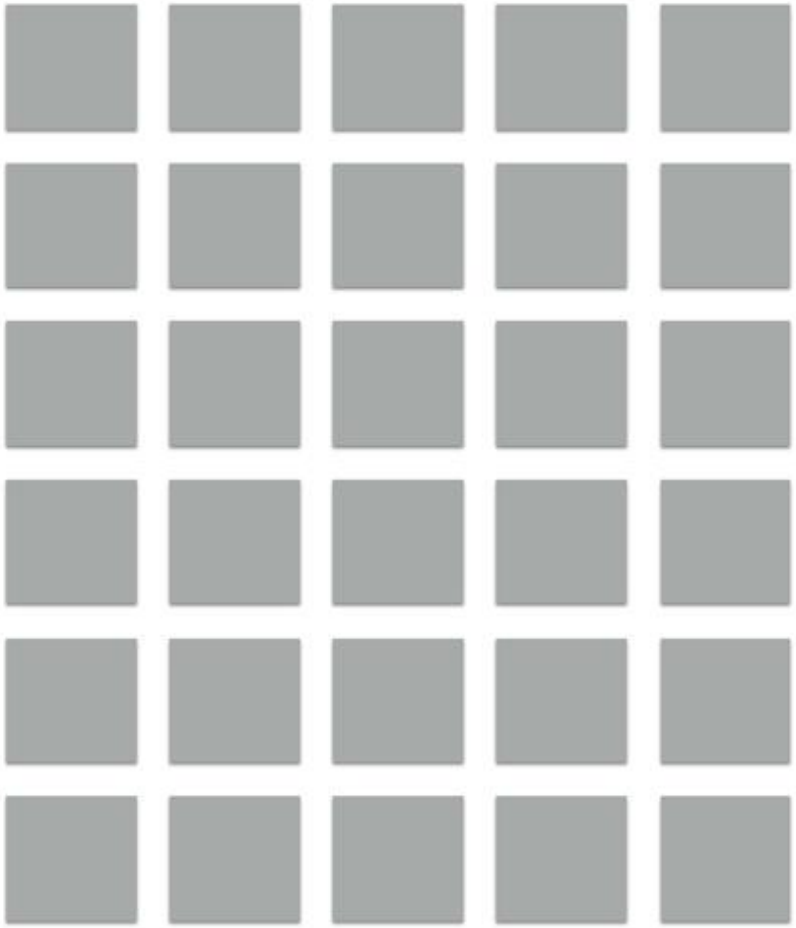
No correlation rules

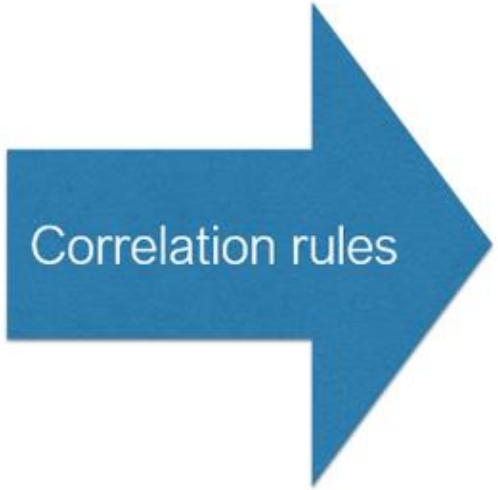


Event correlation

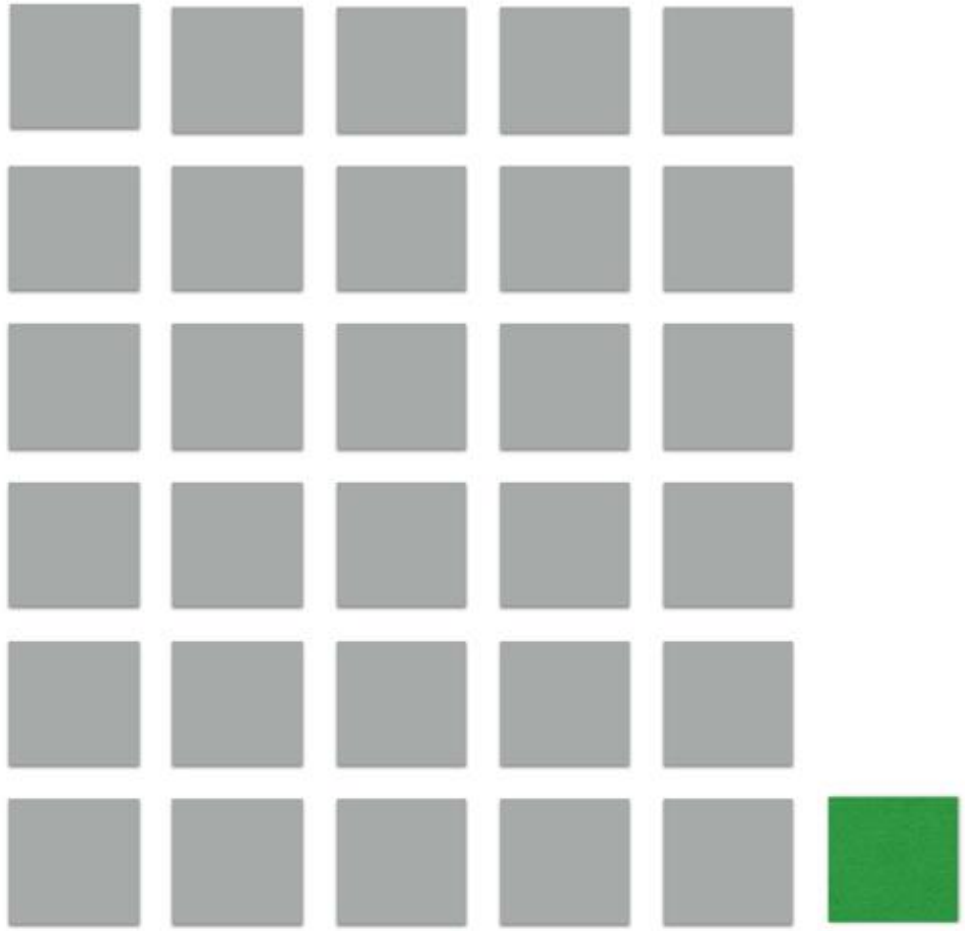
initMAX

Existing problems





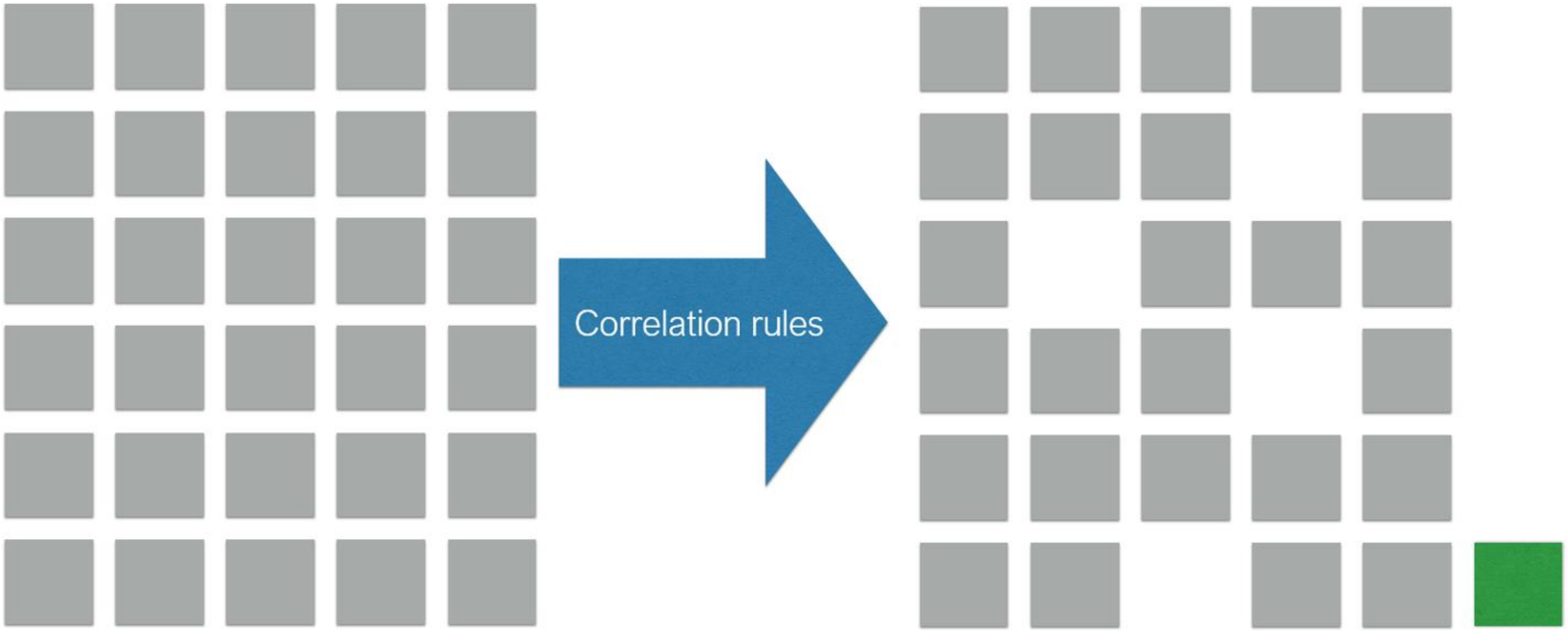
No correlation rules



Event correlation

Existing problems

No correlation rules (close

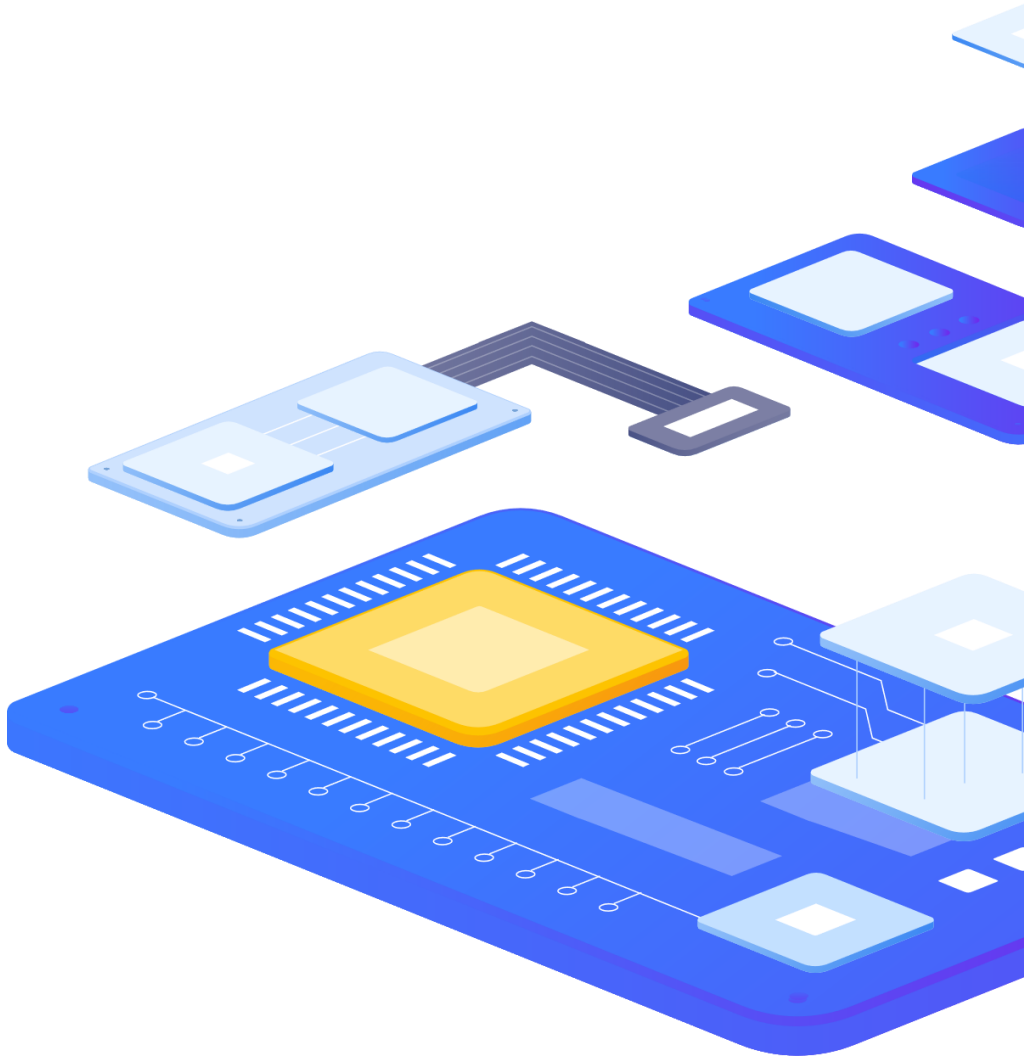


initMAX

ADVANCED PROBLEM DETECTION

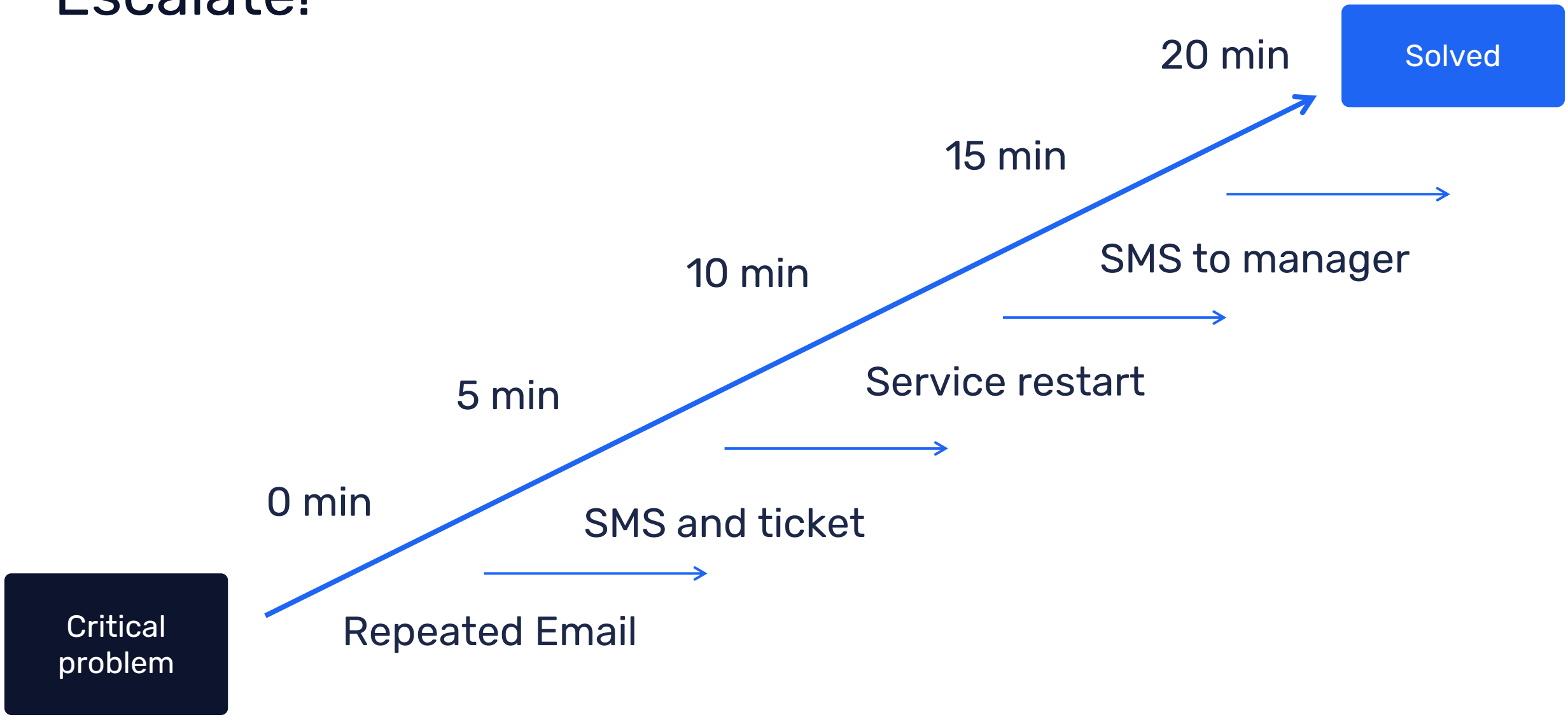
Escalate!

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



ADVANCED PROBLEM DETECTION

Escalate!



initMAX

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

ADVANCED PROBLEM DETECTION

initMAX

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