initMAX

Webinar

Advanced problem detection

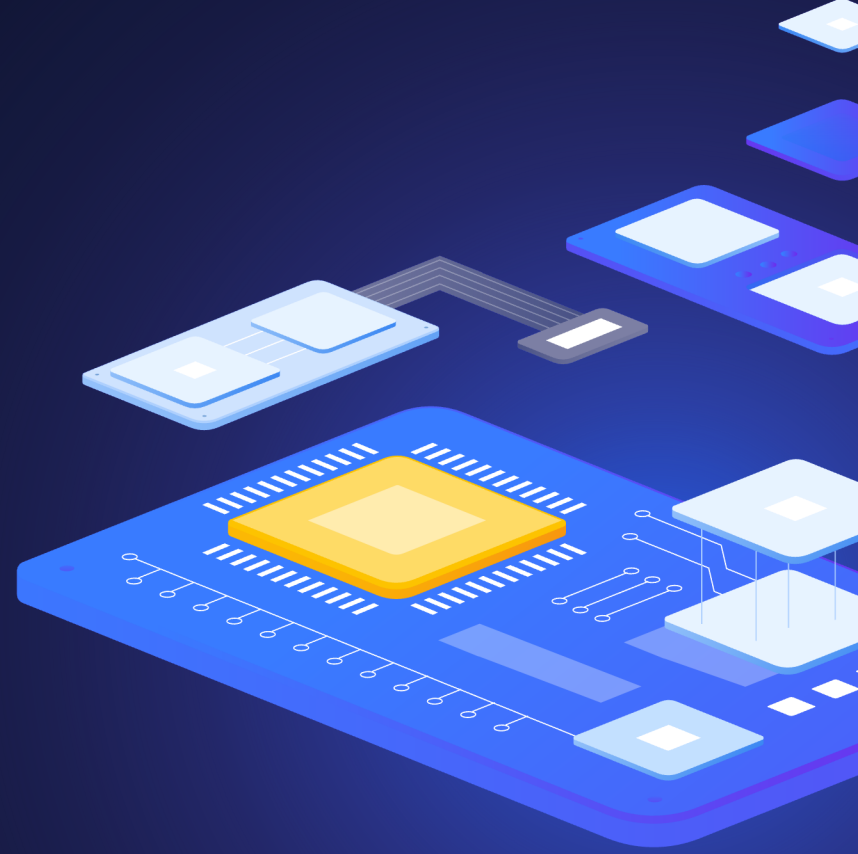
all our microphones are muted

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

use Chat for discussion, networking or applause

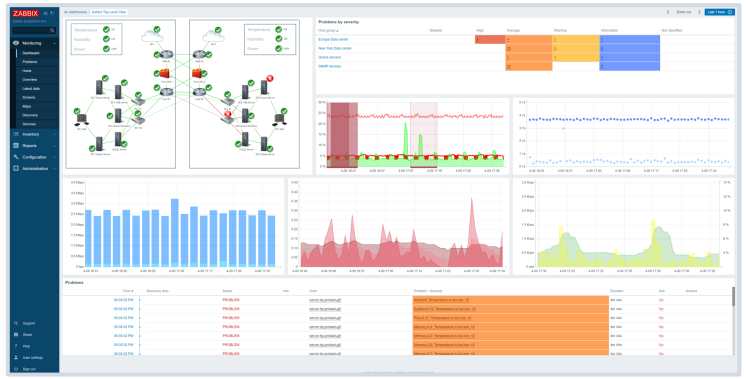
1

Zabbix data flow



ADVANCED PROBLEM DETECTION

Zabbix data flow

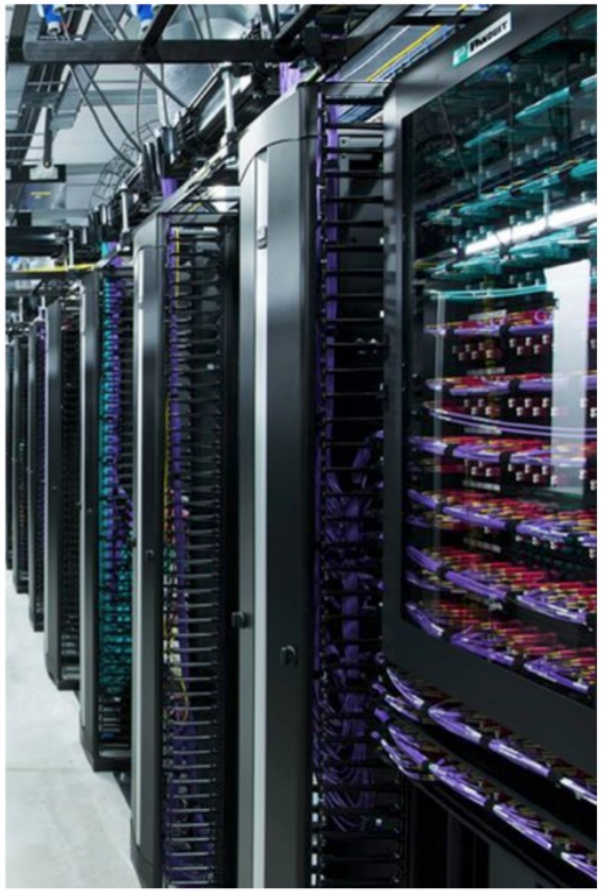


Visualization

Notifications

DATABASE

ZABBIX SERVER



History

Analysis

Data collection

initMAX

How often to execute checks?

Every N seconds

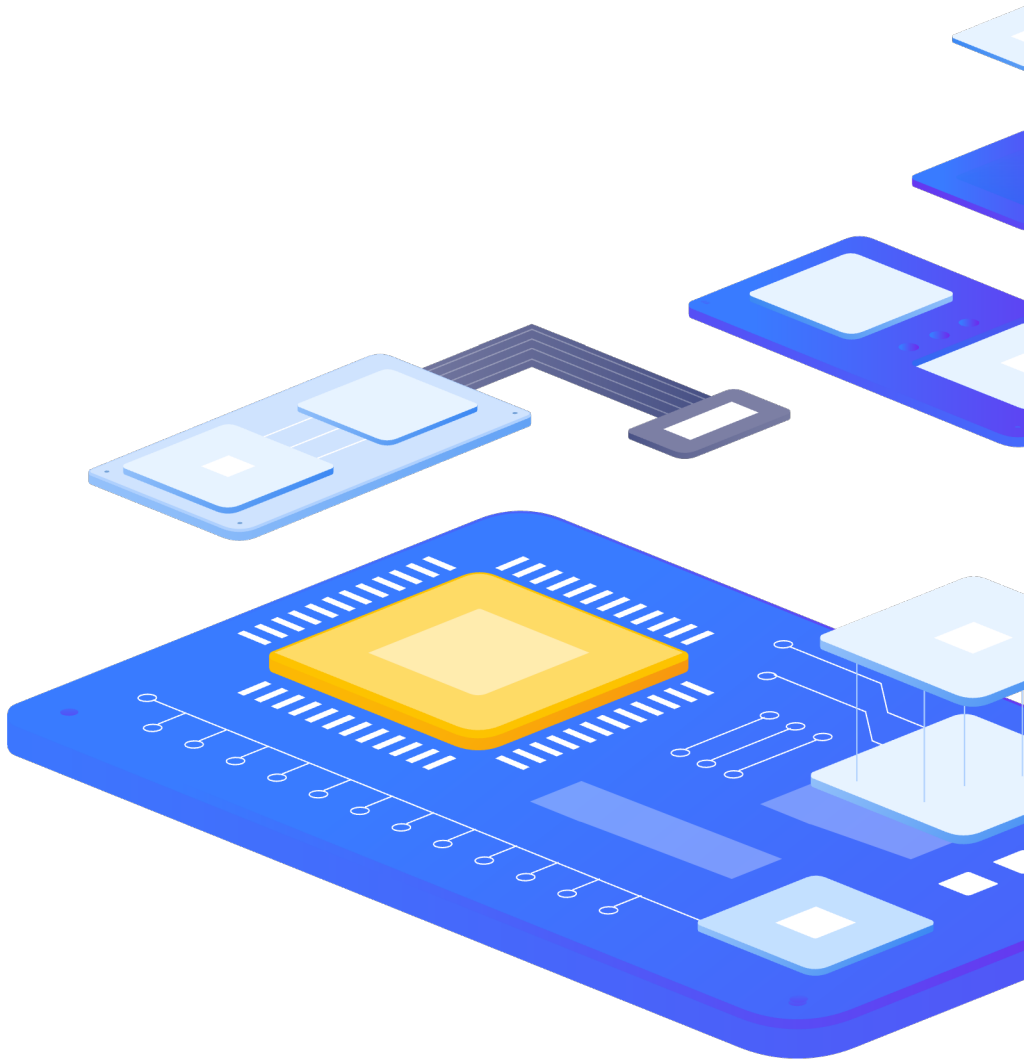
- Zabbix will evenly distribute checks

Different frequency in different time periods

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

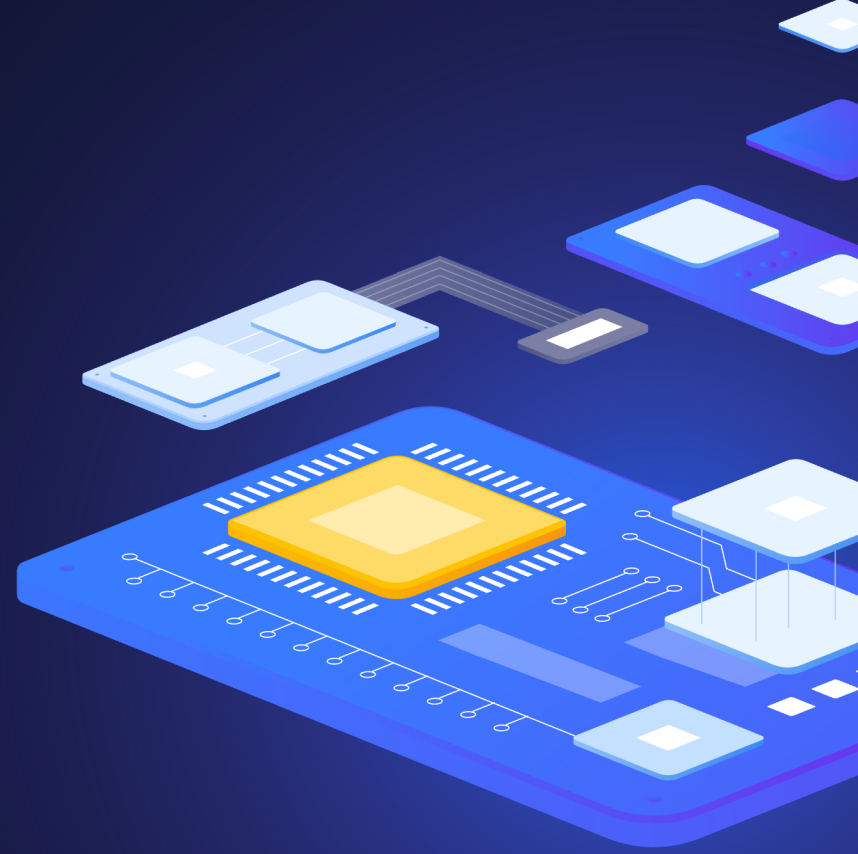
At a specific time (Zabbix 3.0)

- 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

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

Scope of Usage

- Triggers, calculated items, expression macros

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	change, changecount, count, countunique, find, first, fuzzytime, last, logeventid, logseverity, logsource, monodec, monoinc, nodata, percentile, rate
Trend functions	baselinedev, baselinewma, 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)

TAG level

- avg_foreach(/*/key[a,*,c]?[(tag=„ENV:production")],10m)

Complex level

- avg_foreach(/*/key[a,*,c]?[(group=„Servers" and tag=„EU") or (group=„Linux„) and (tag=„CZ" or tag=„ENV:production"))],5m)

initMAX

Zabbix 7.0

jsonpath(value,path,<default>)

Return the JSONPath result.

Supported value types: String, Text, Log.

- jsonpath(last(/host/proc.get[zabbix_agentd,,,summary]),"$..size")

xmlxpath(value,path,<default>)

Return the XML XPath result.

Supported value types: String, Text, Log.

- xmlxpath(last(/host/xml_result),"/response/error/status")

initMAX

Zabbix 7.0

Updated functions

- Aggregate functions now also support non-numeric types for calculation. This may be useful, for example, with the count and count_foreach functions.
- The count and count_foreach aggregate functions support optional parameters operator and pattern, which can be used to fine-tune item filtering and only count values that match given criteria.
- All foreach functions no longer include unsupported items in the count.
- The function last_foreach, previously configured to ignore the time period argument, accepts it as an optional parameter.
- Supported range for values returned by prediction functions has been expanded to match the range of double data type. Now timeleft() function can accept values up to 1.7976931348623158E+308 and forecast() function can accept values ranging from -1.7976931348623158E+308 to 1.7976931348623158E+308.

initMAX

ADVANCED PROBLEM DETECTION

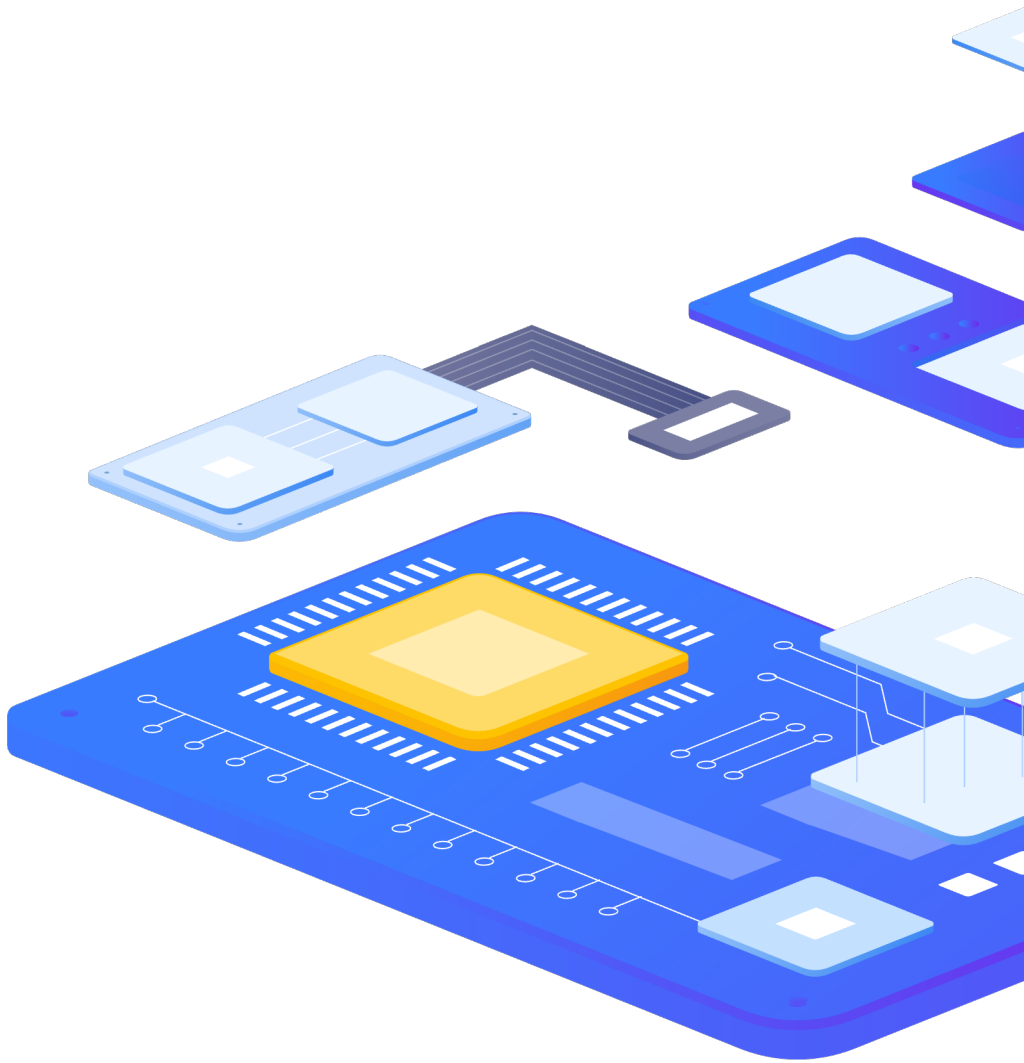
Junior level

Performance

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

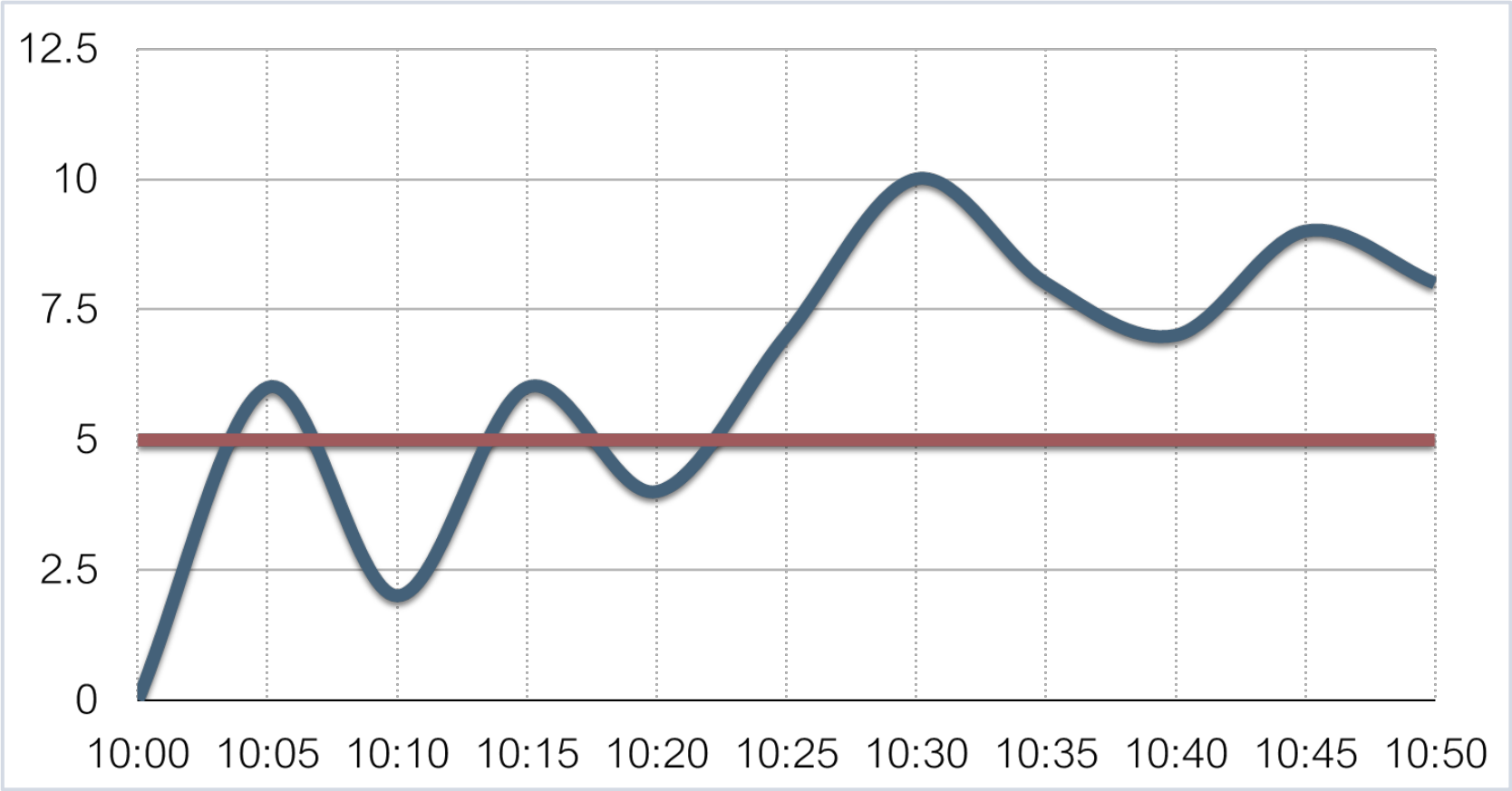
Availability

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



initMAX

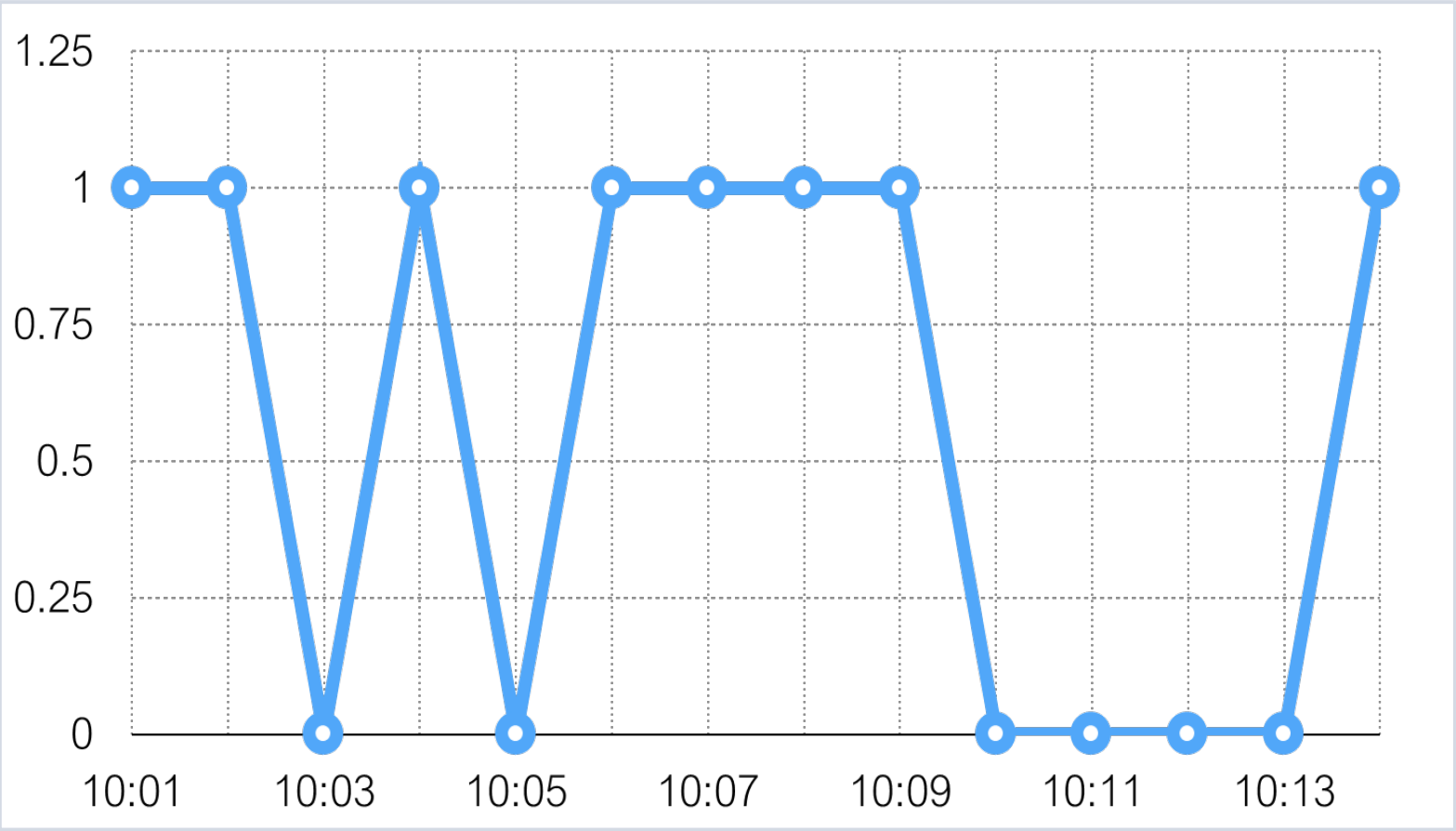
False positives



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

ADVANCED PROBLEM DETECTION

Too sensitive



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

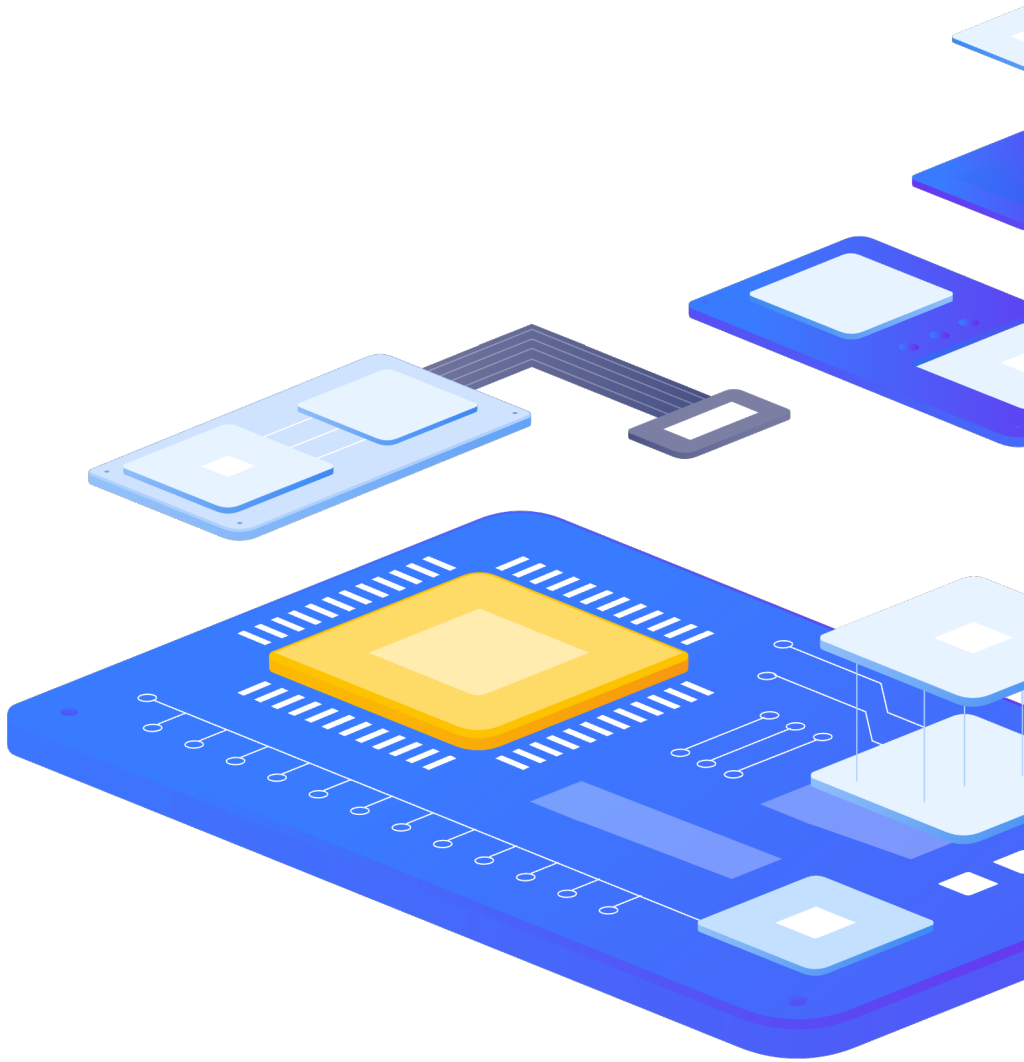
initMAX

Advanced problem detection

Junior level

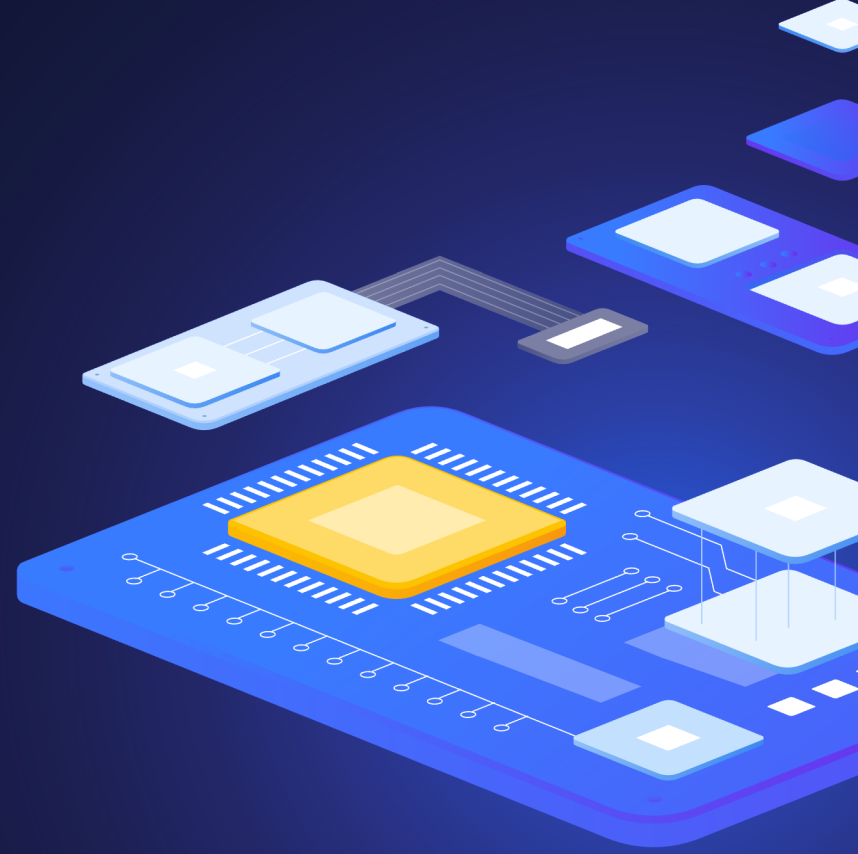
Too sensitive leads to

- False positives



3

False positives



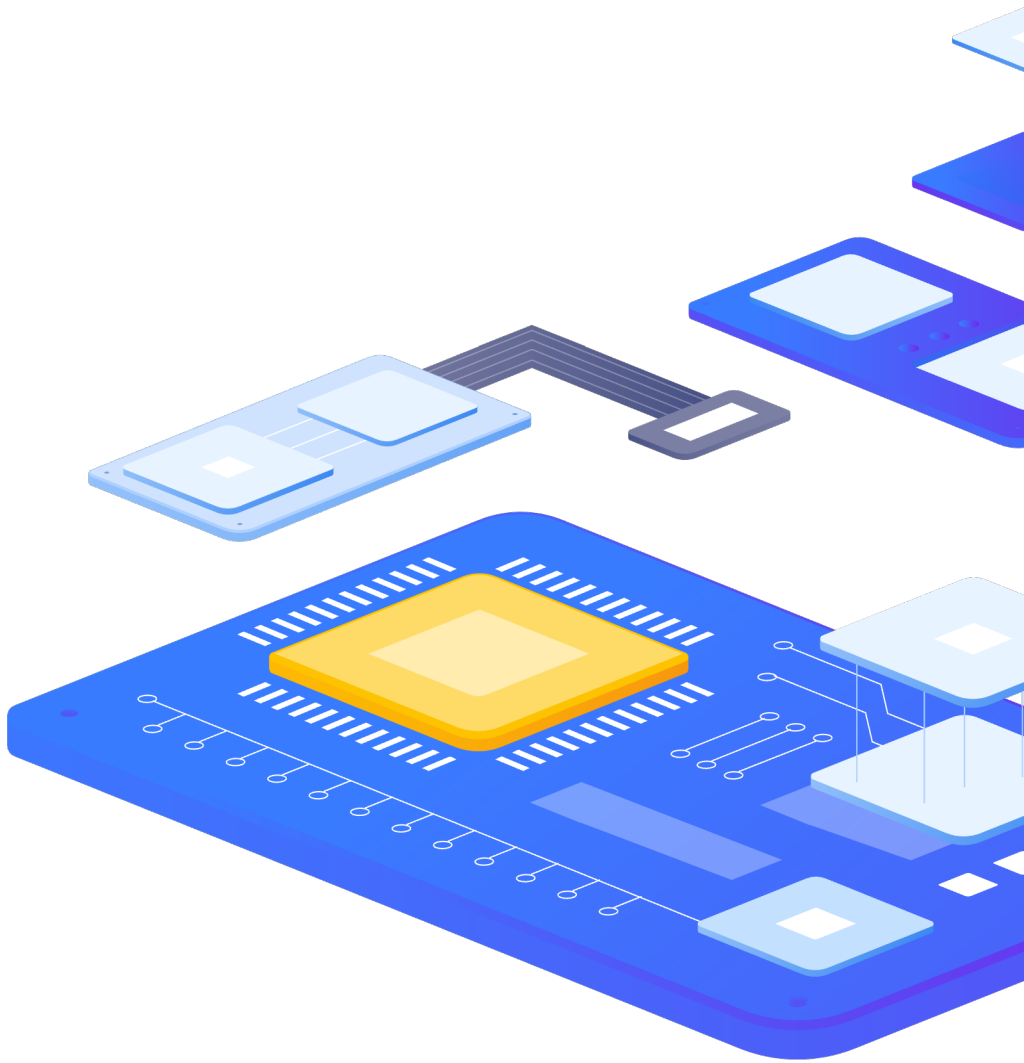
initMAX

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?**

initMAX

Analyze history

Performance

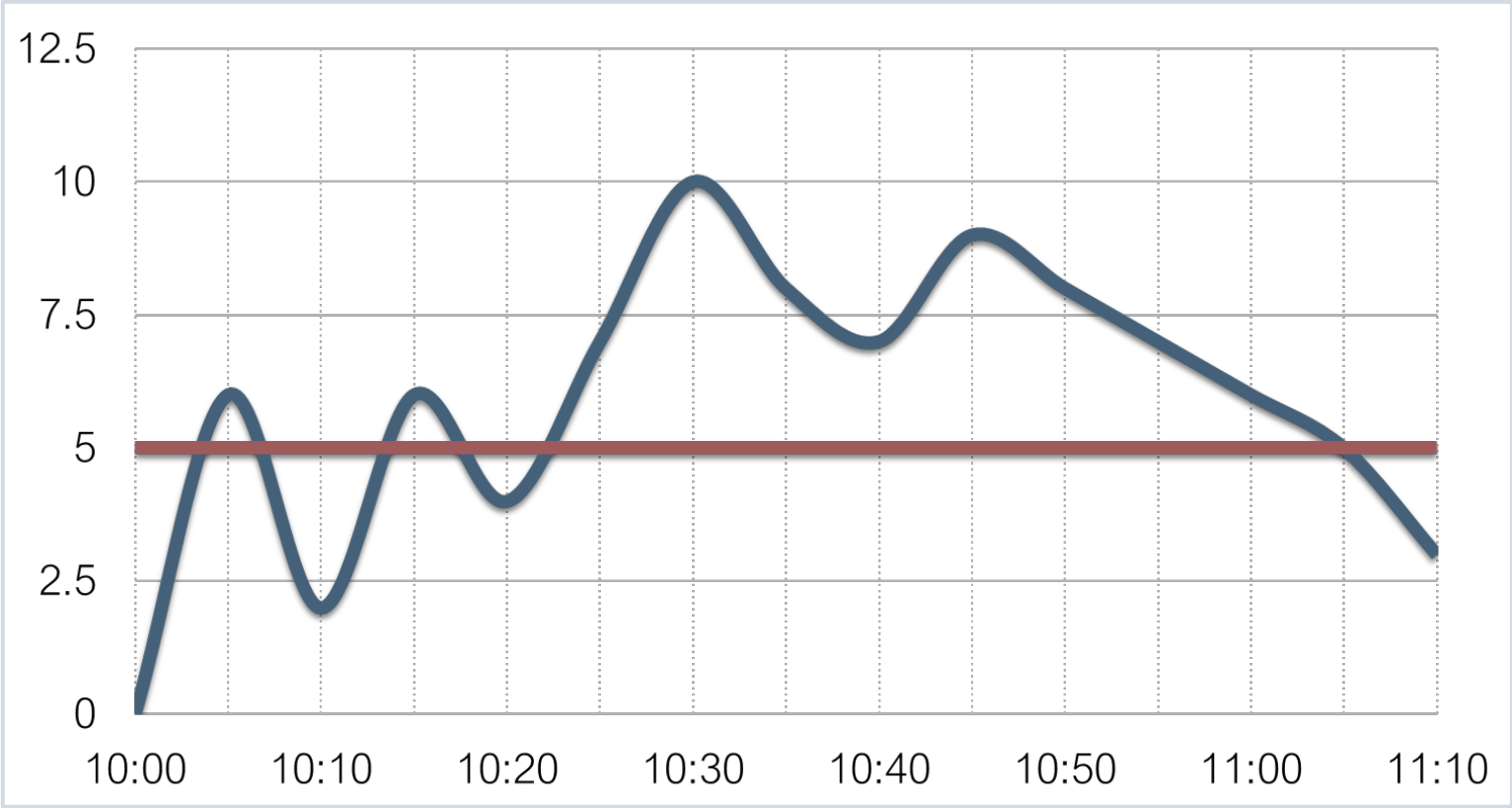
- min(/server/system.cpu.load,10m) > 5

Availability

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

initMAX

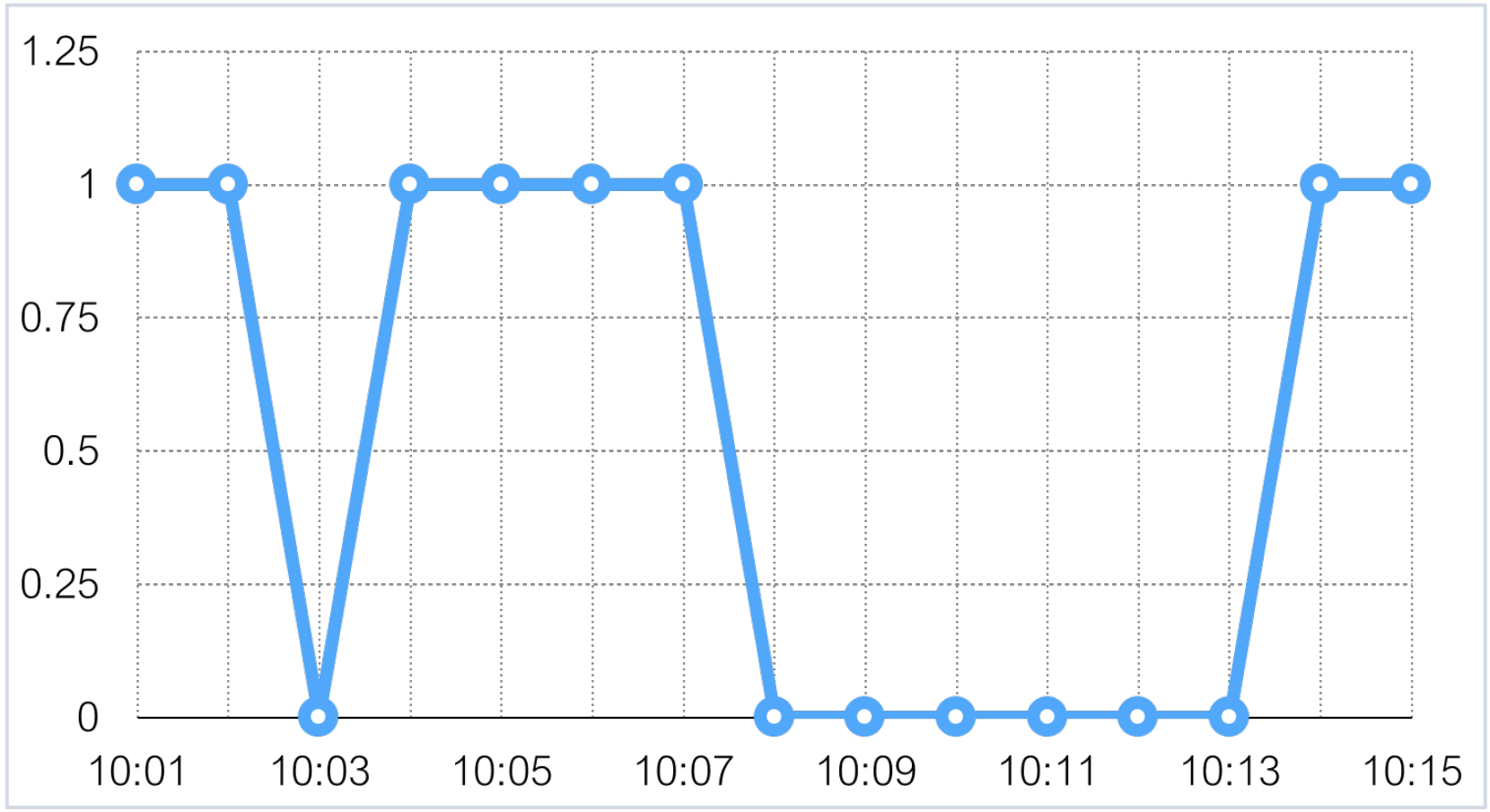
Analyze history



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

ADVANCED PROBLEM DETECTION

Analyze history



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

ADVANCED PROBLEM DETECTION

Different conditions for problem and recovery

Before

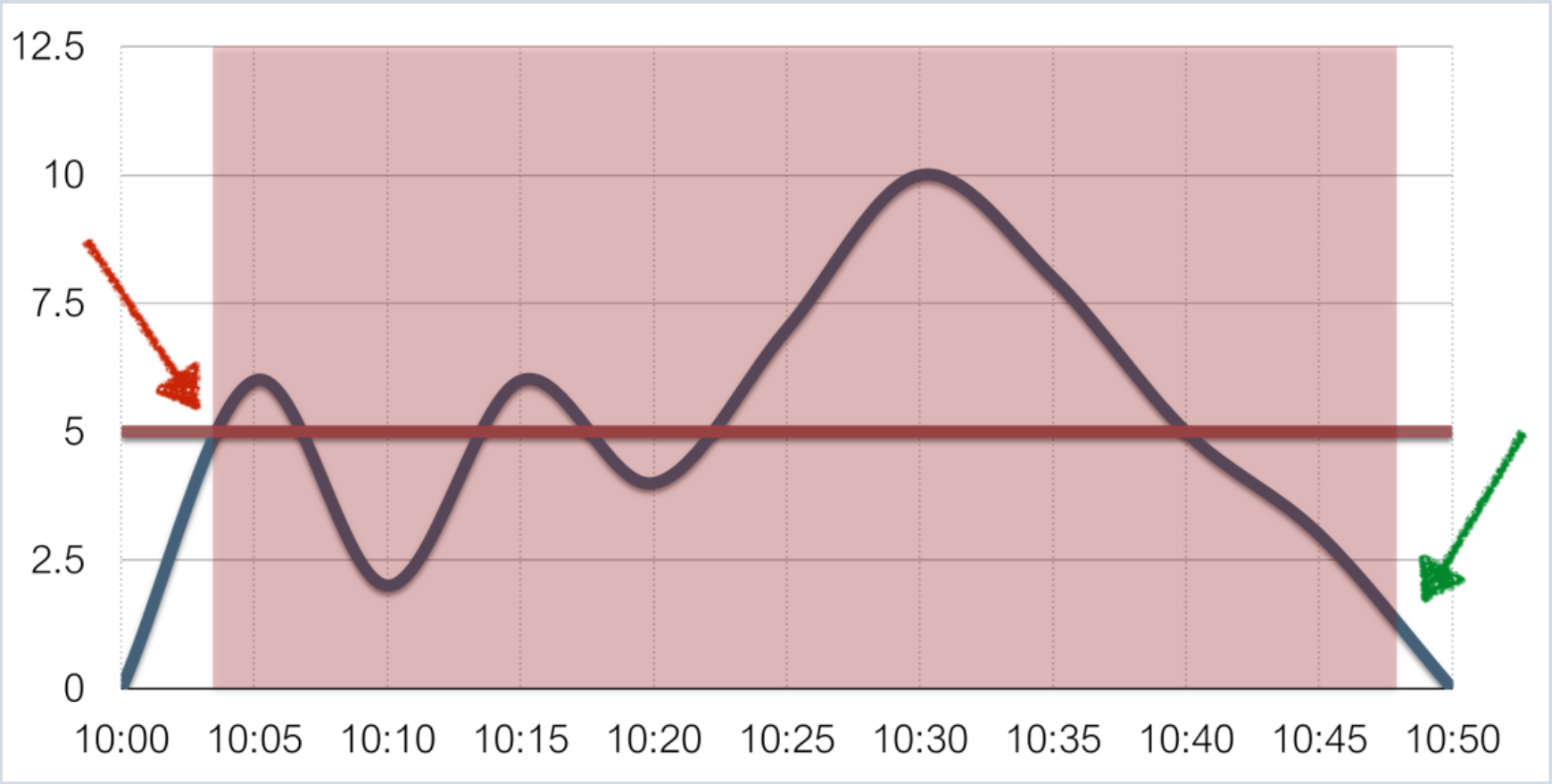
- last(/server/system.cpu.load) > 5

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

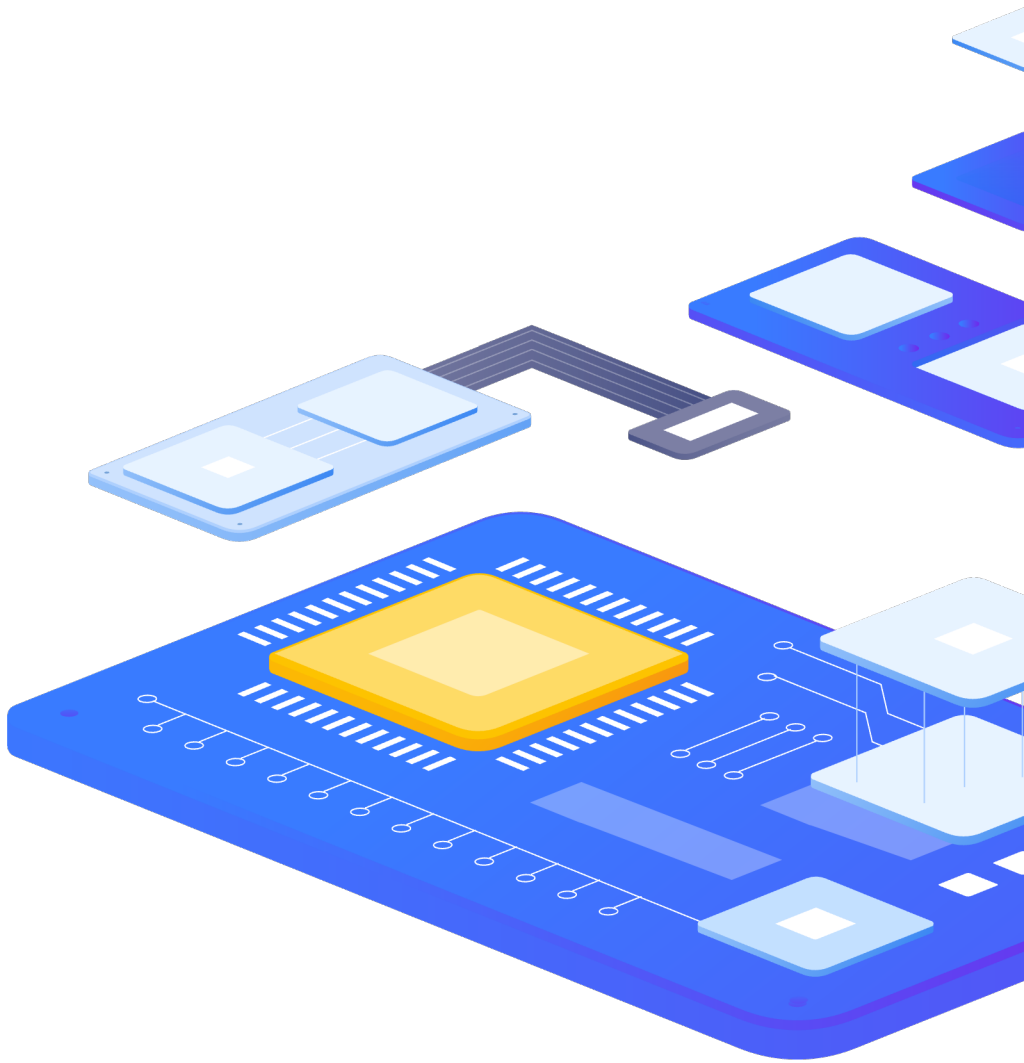
No free disk space /

Problem definition:

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

Recovery expression:

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



Examples

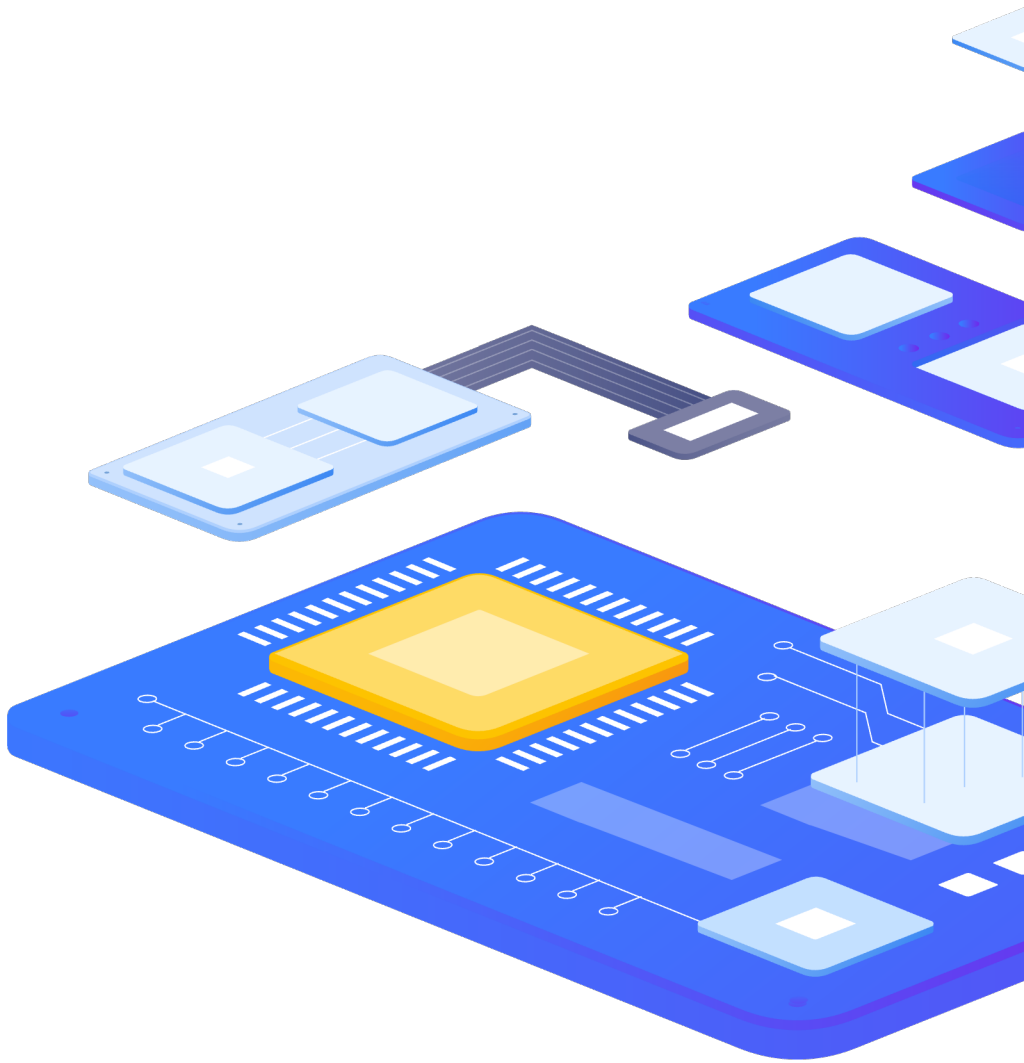
SSH is not available

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.

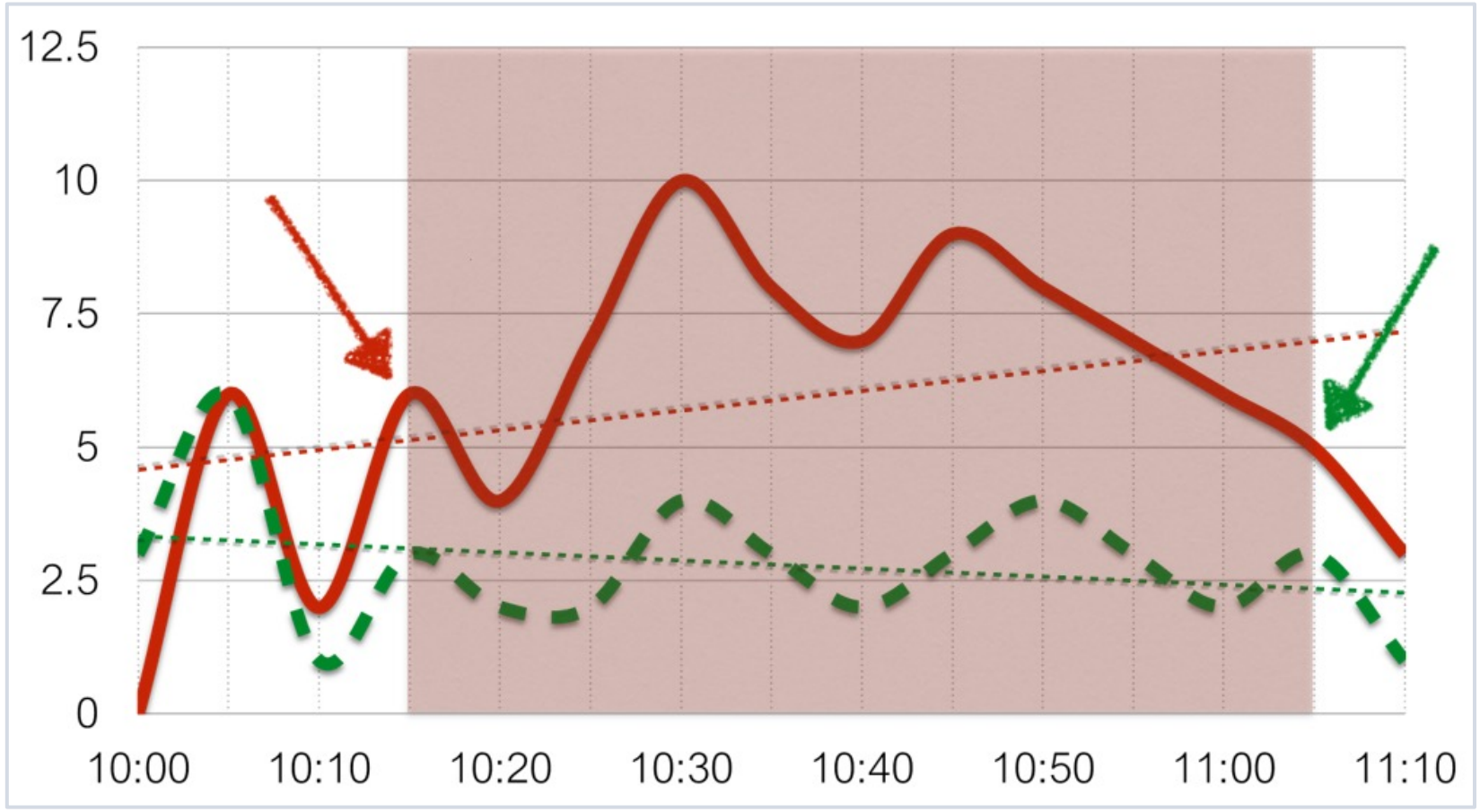
Average CPU load for the last hour is 2x higher than

CPU load for the same period week ago

- avg(/server/system.cpu.load,1h) > 2* avg(/server/system.cpu.load,1h:now-7d)

ADVANCED PROBLEM DETECTION

Anomalies



Comparison with the data 7 days ago

ADVANCED PROBLEM DETECTION

Flapping

How to detect?

By comparing changecount of the data from the time period.

Operational status changes of interface

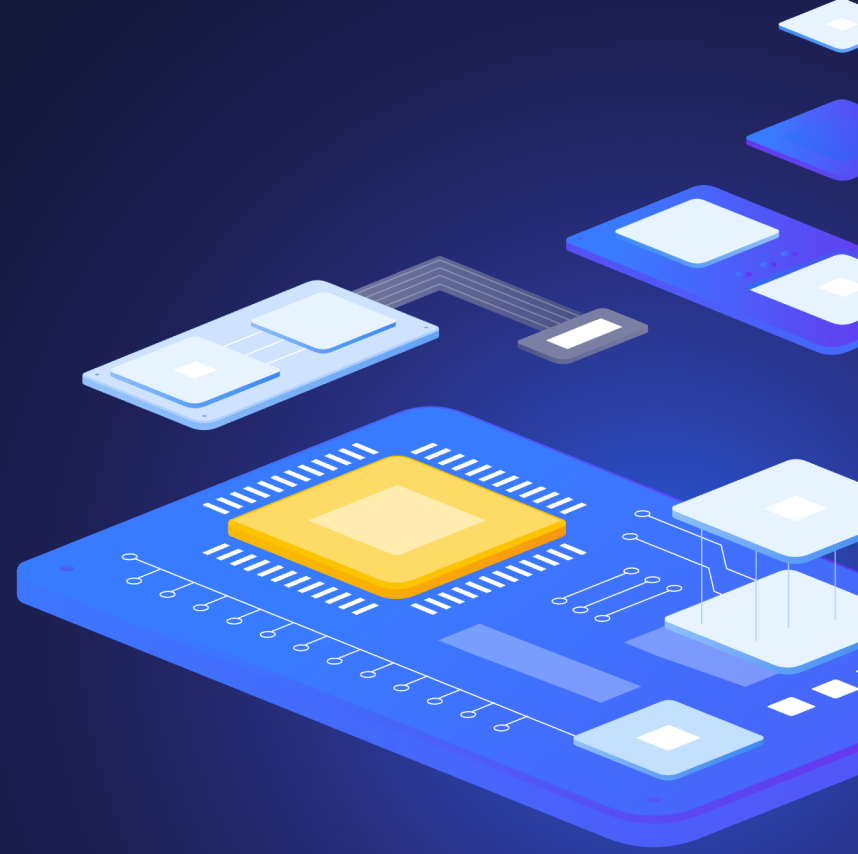
- changecount(/SNMP v2/net.if.status[ifOperStatus.{#SNMPINDEX}],{$FLAP.PERIOD})>{$FLAP.NUMBER}

Trigger dependency

Link down -> Flapping Detected

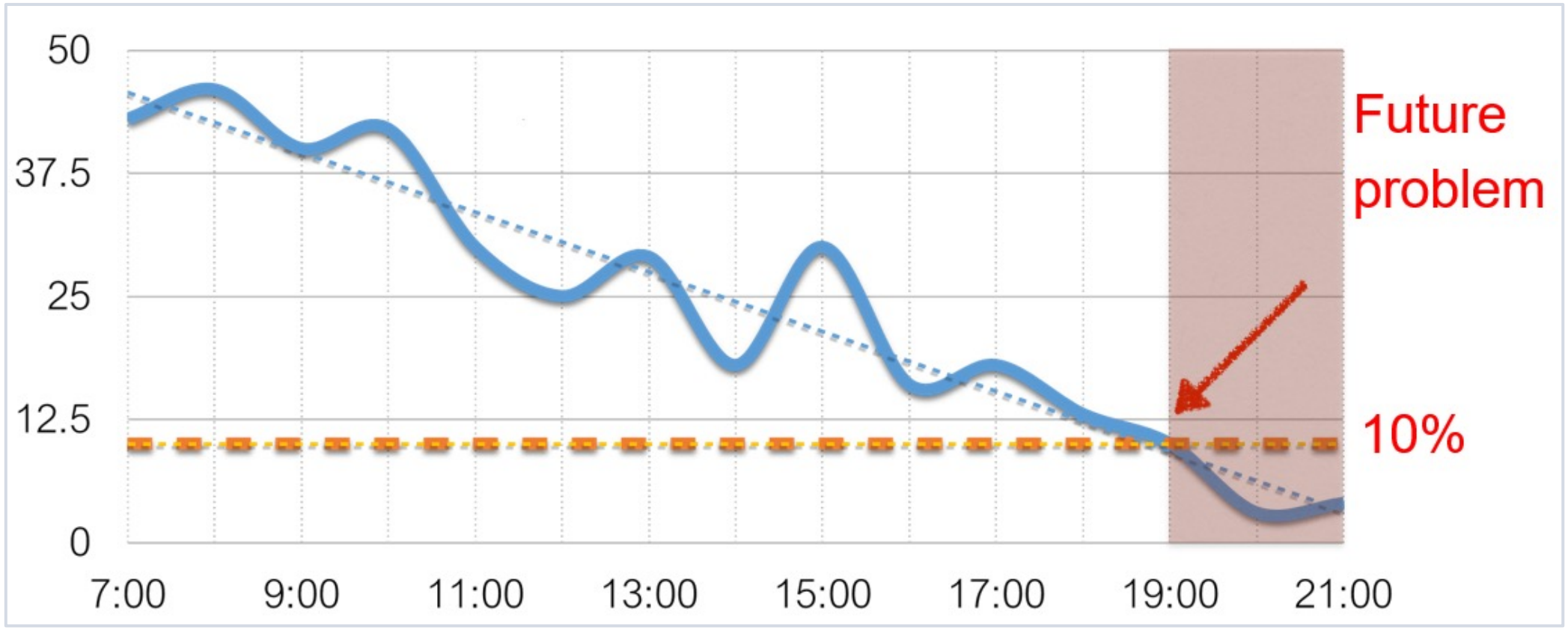
3

Forecast



ADVANCED PROBLEM DETECTION

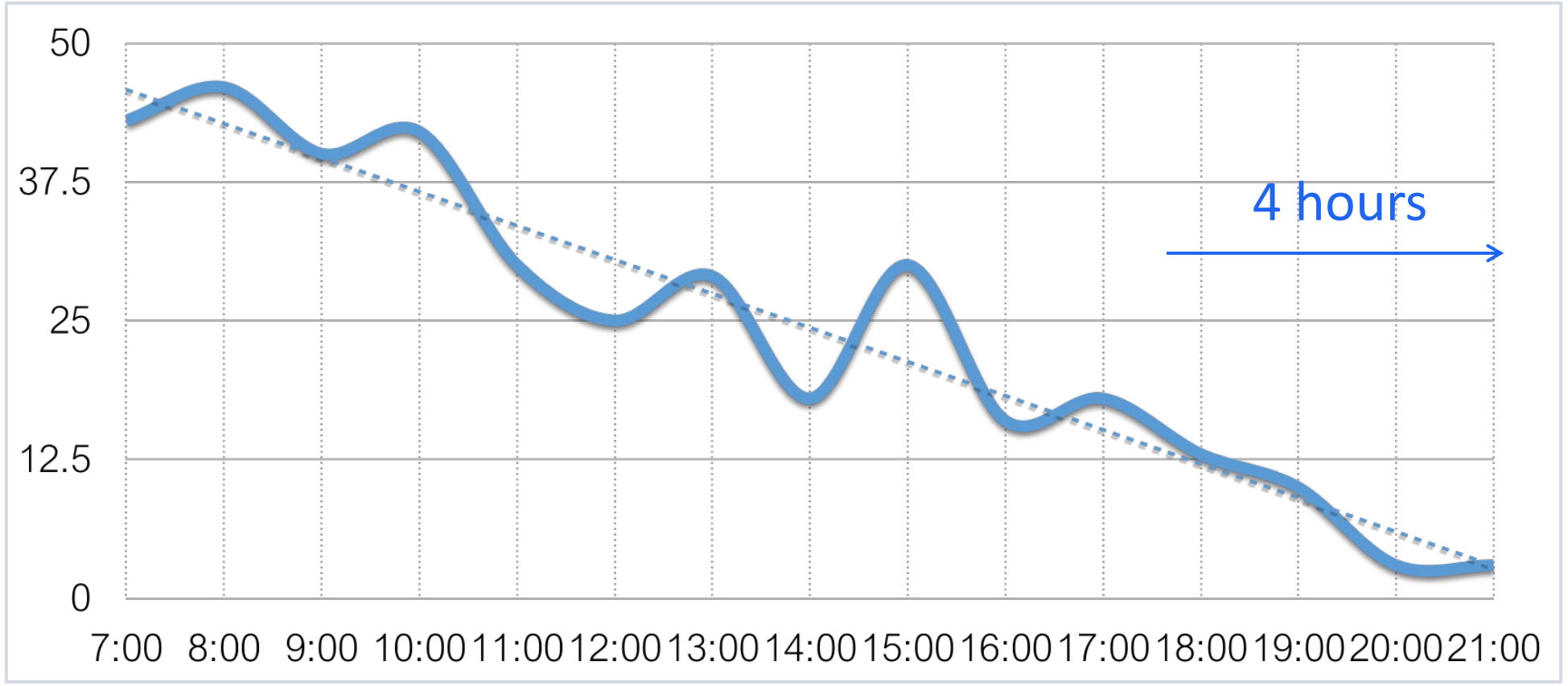
Forecast



Trigger function timeleft

ADVANCED PROBLEM DETECTION

Forecast



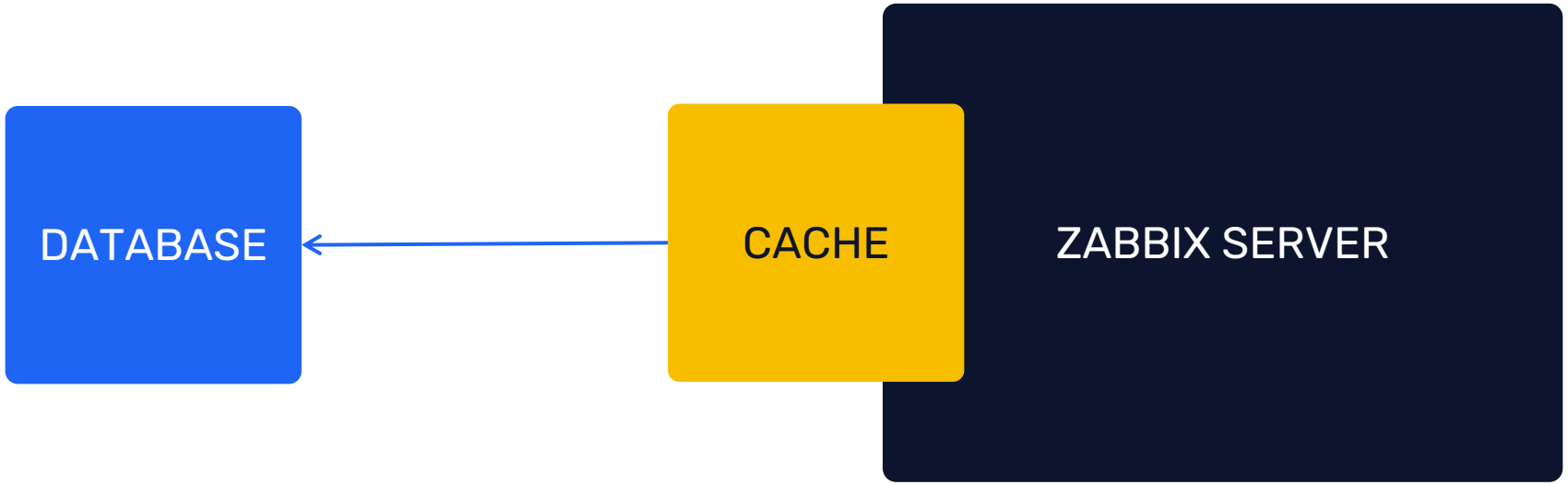
Trigger function forecast

initMAX

Does history analysis affect performance of Zabbix?

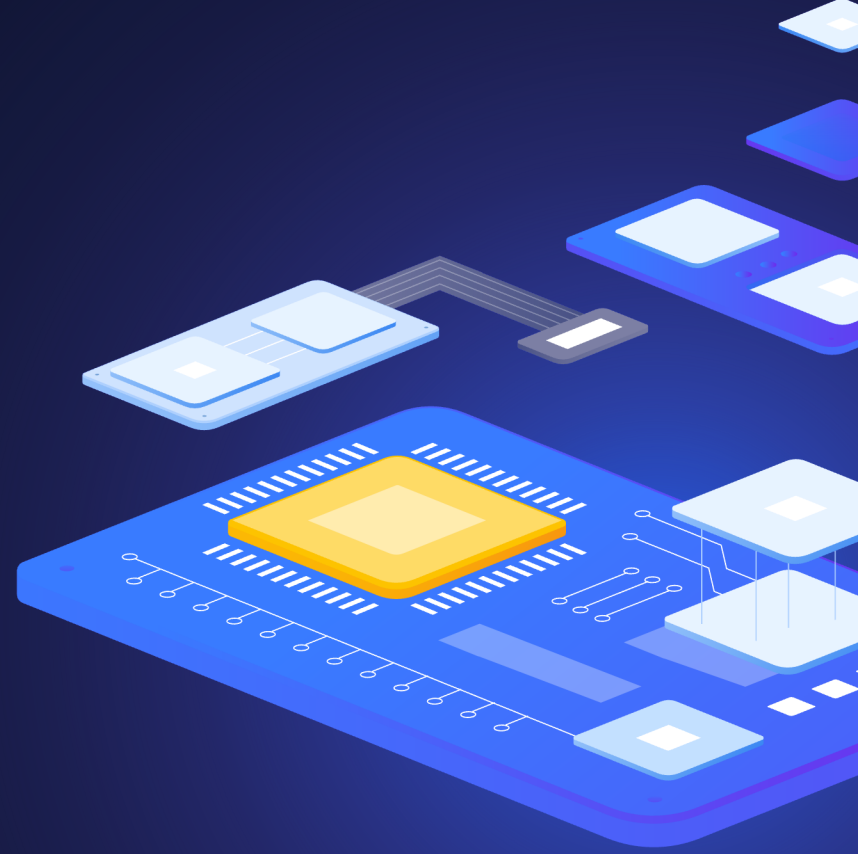
Yes, but not significantly.

Especially as of Zabbix 2.2.0.



4

Dependencies



initMAX

ADVANCED PROBLEM DETECTION

Dependencies

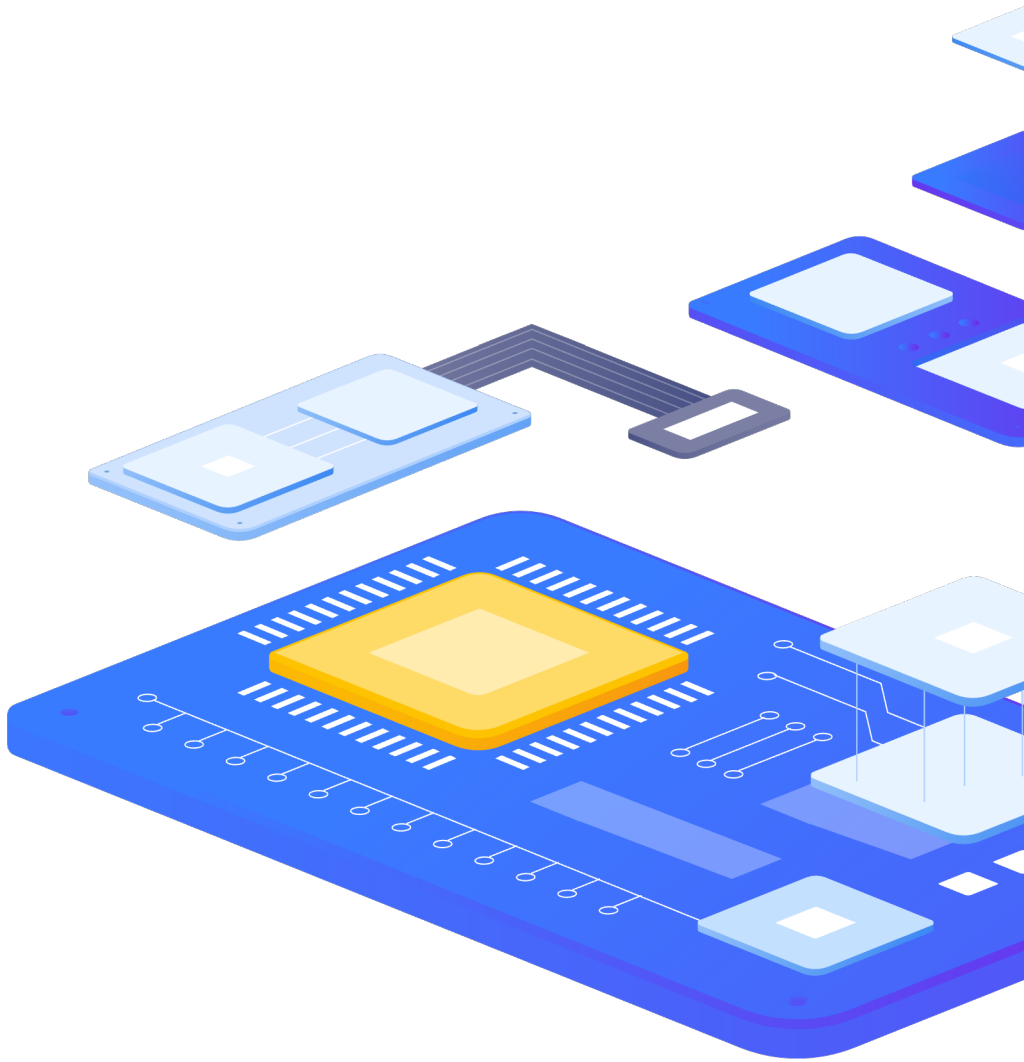
CRM is not working

↓

DB is unavailable

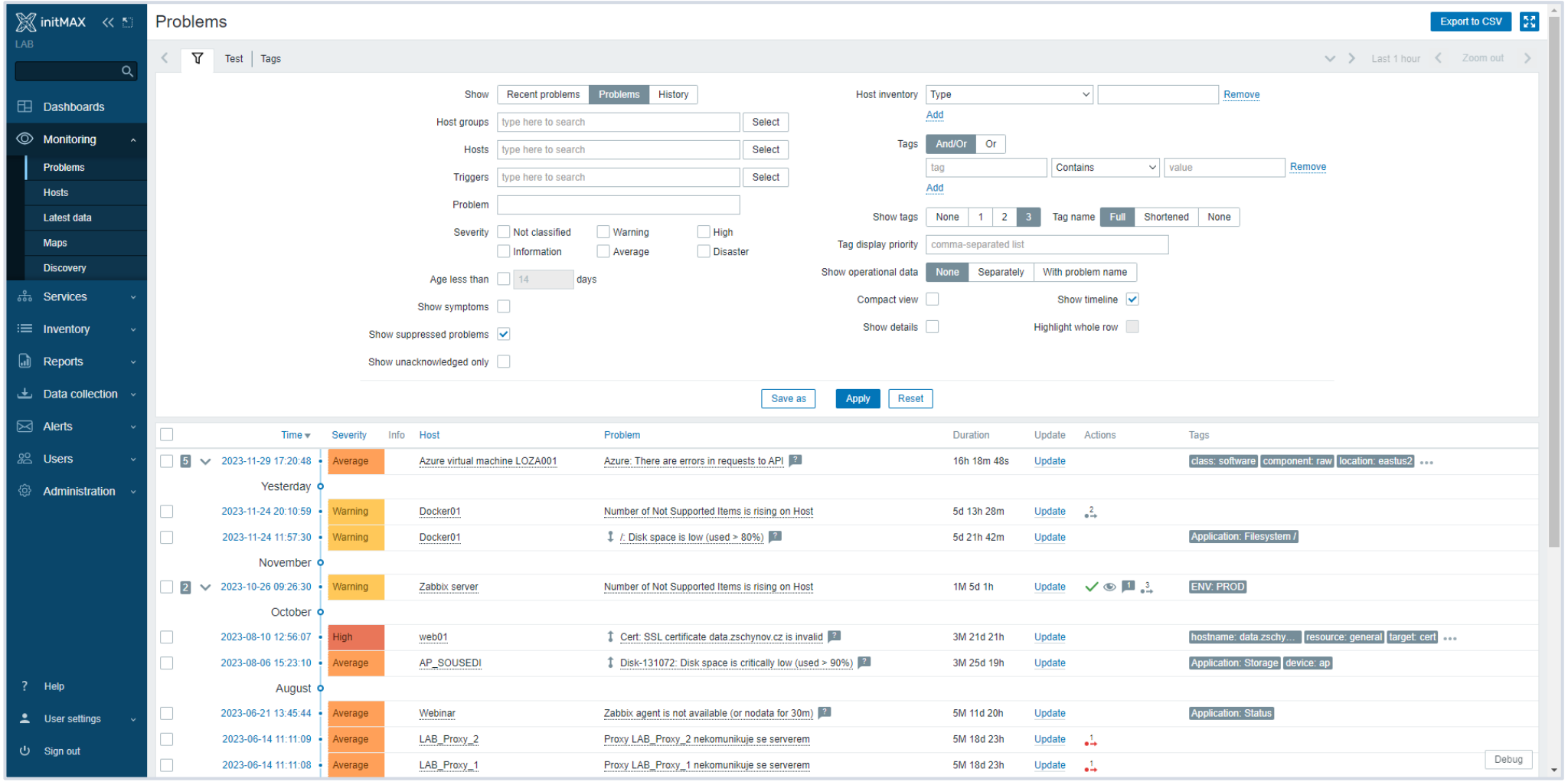
↓

No free diskspace



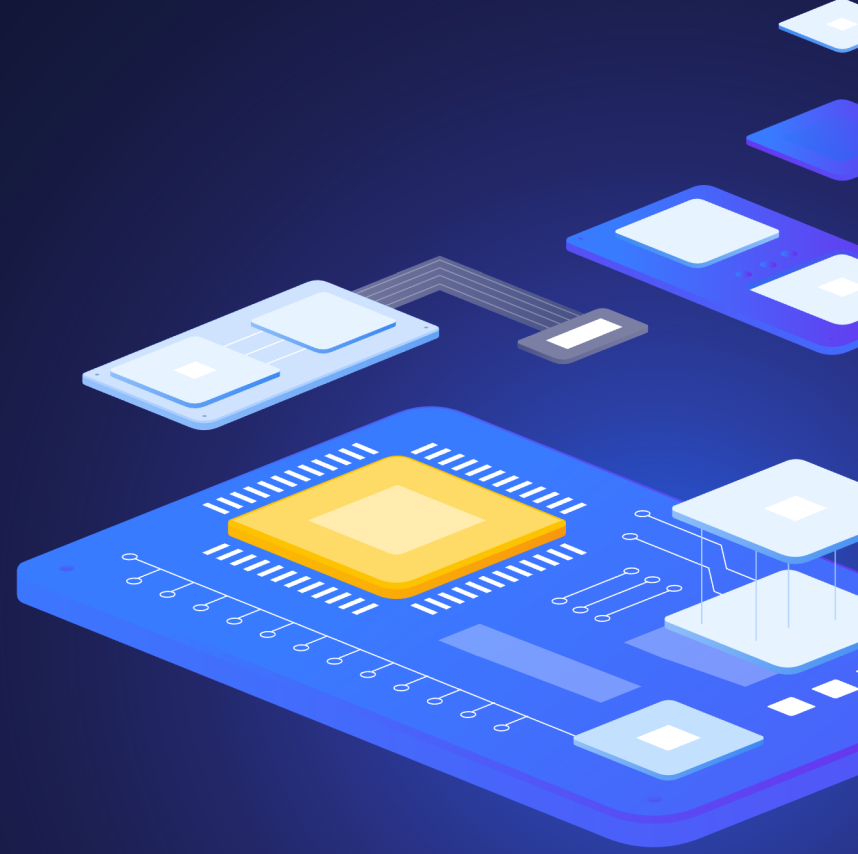
ADVANCED PROBLEM DETECTION

Section „Problems“



5

Tags



initMAX

Tags

Tag word: meaning

Customer: Alza
Customer: Globus

Datacenter: NY2
Datacenter: San Francisco

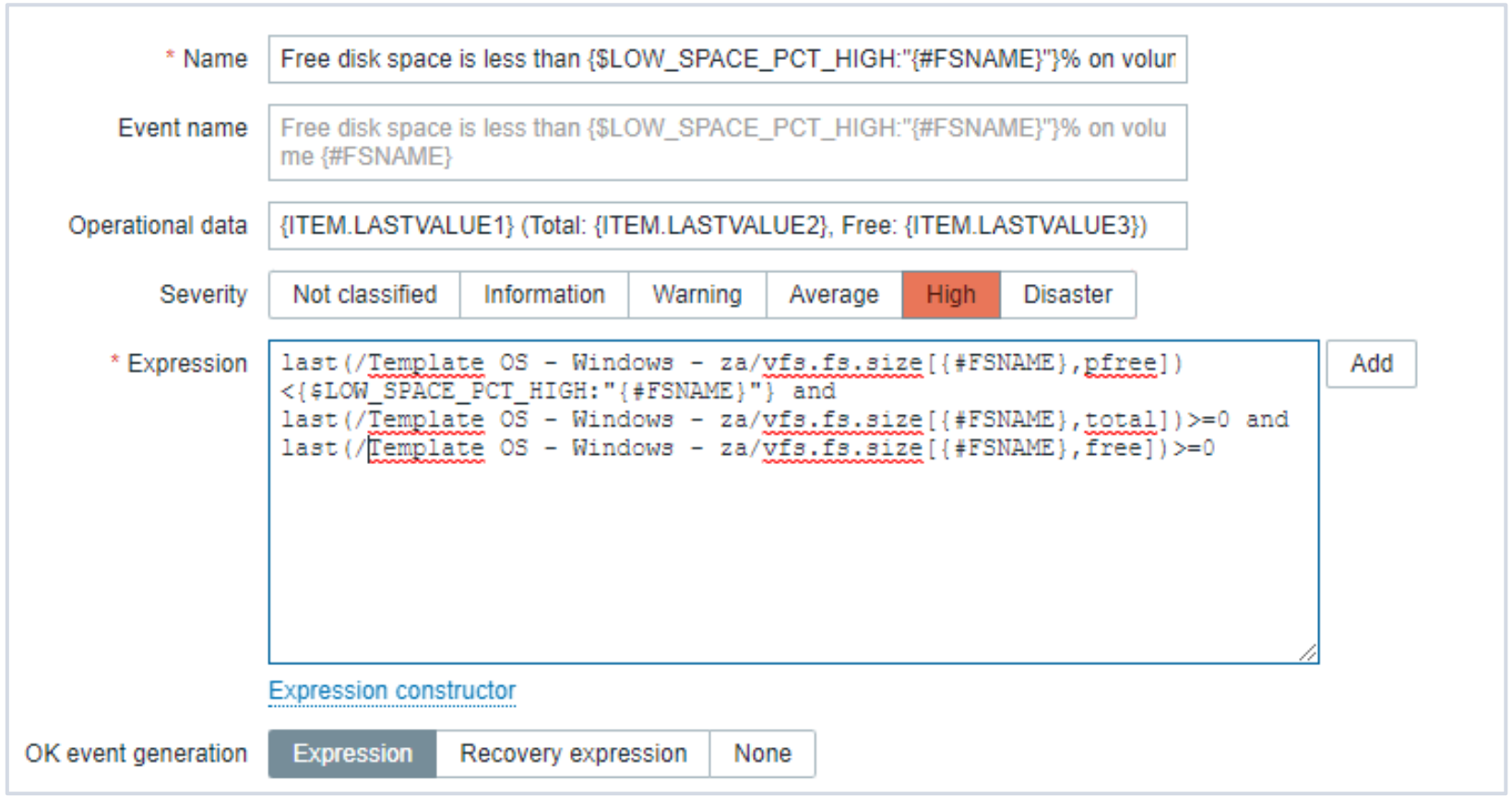
Area: Performance
Area: Availability
Area: Security

Environment: Staging
Environment: Test

User impact: None
User impact: Critical

Use of obtained values

Use of useful information in tags or names



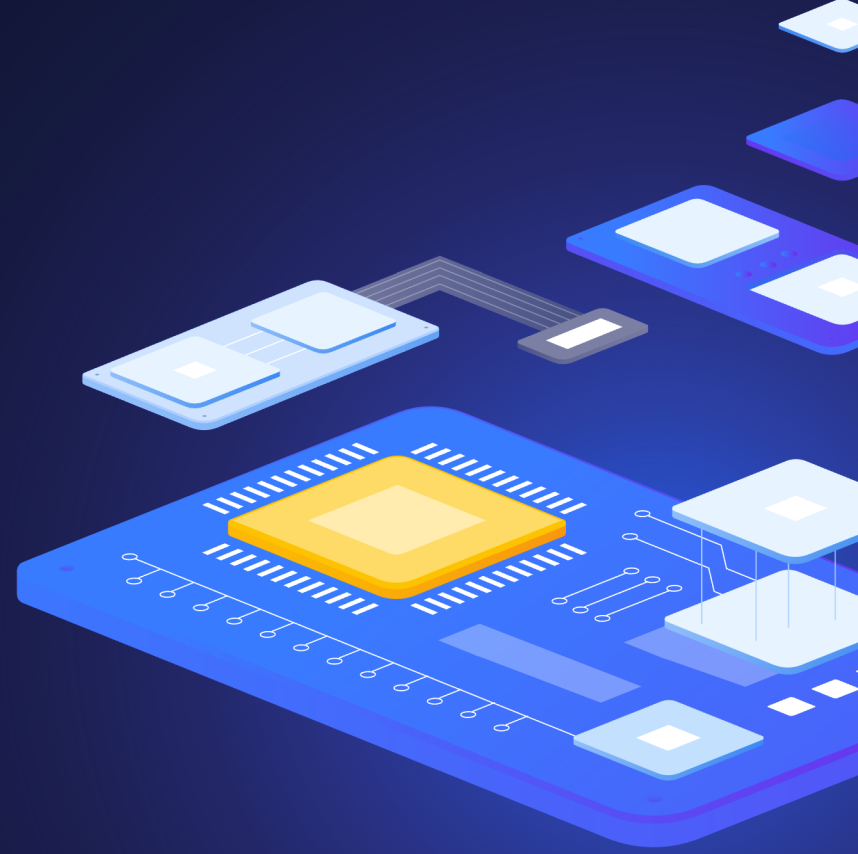
ADVANCED PROBLEM DETECTION

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

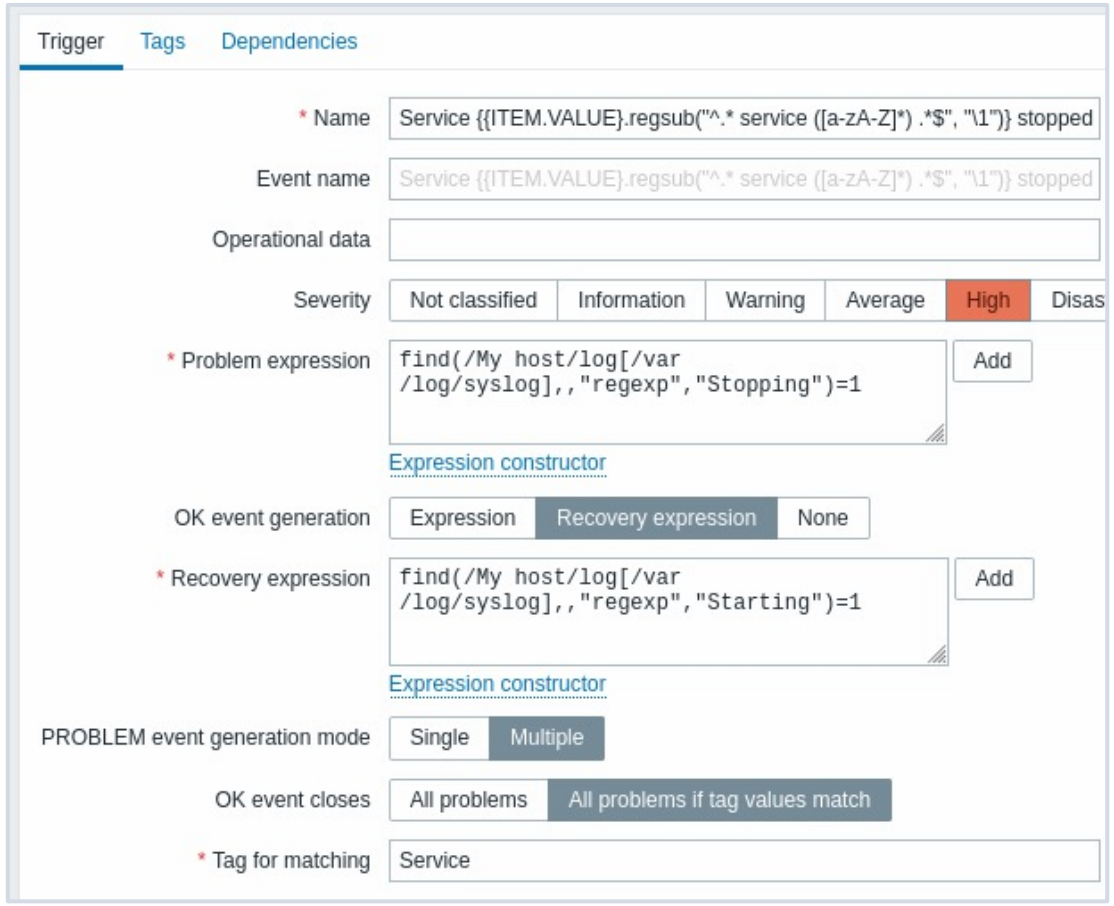
6

Event correlations

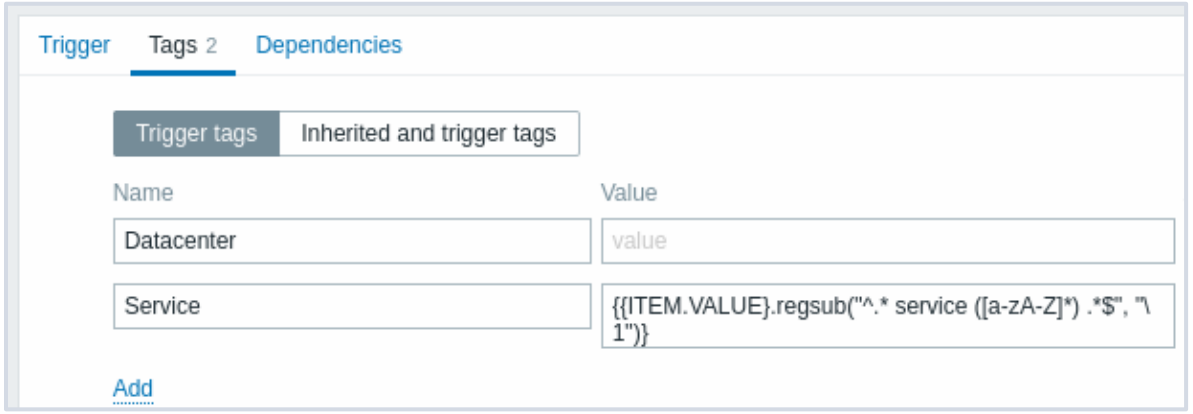


initMAX

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

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

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

initMAX

How does it work?

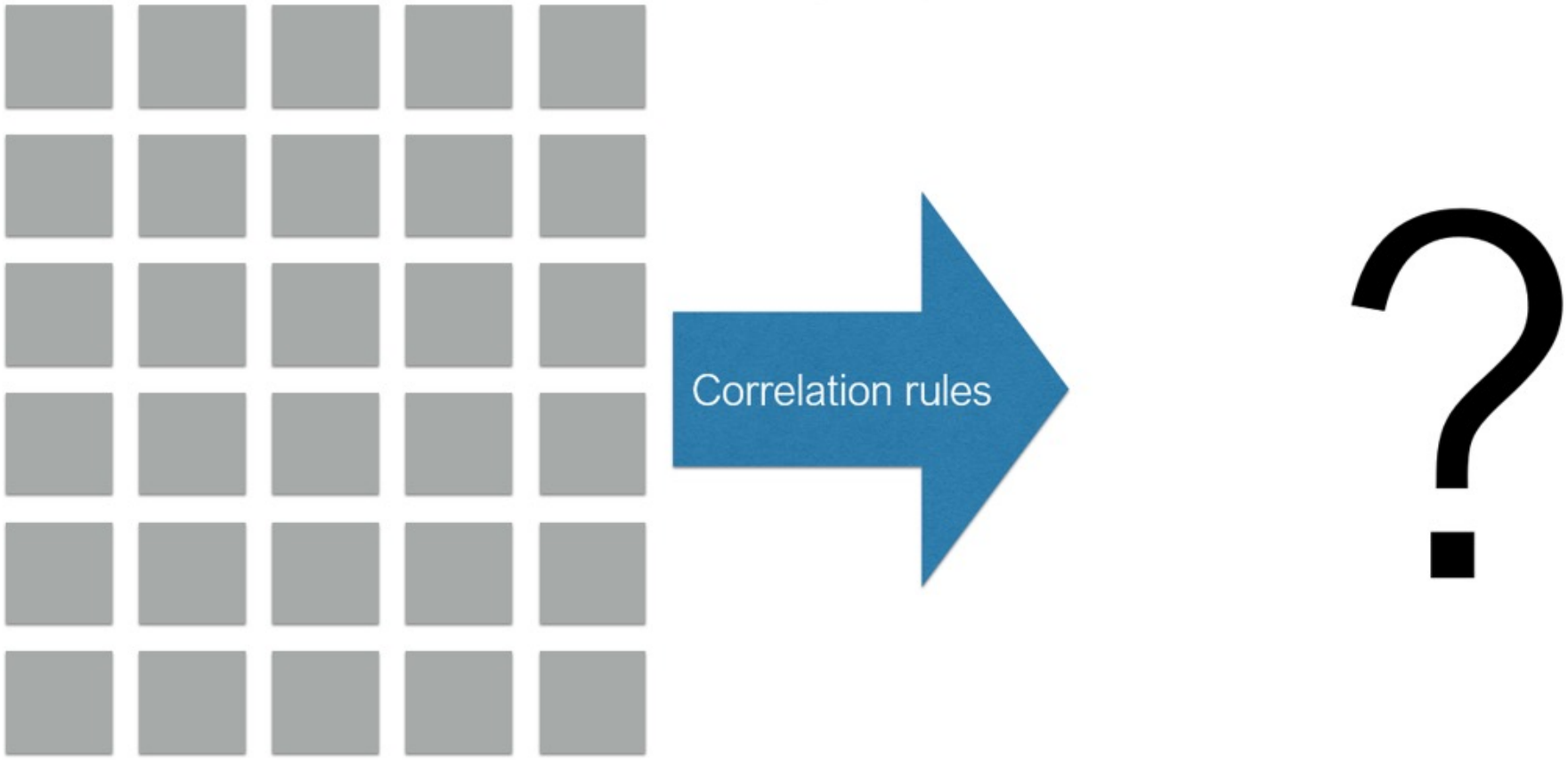
10/Feb/2022:06:25:30 service Jira stopped	“Service Jira stopped”	RESOLVED
10/Feb/2022:06:27:32 service MySQL stopped	“Service MySQL stopped”	RESOLVED
10/Feb/2022:06:28:11 service MySQL started		
10/Feb/2022:06:34:22 service Redis stopped	“Service Redis stopped”	RESOLVED
10/Feb/2022:06:37:58 service Redis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

initMAX

Event correlation

A new problem appears

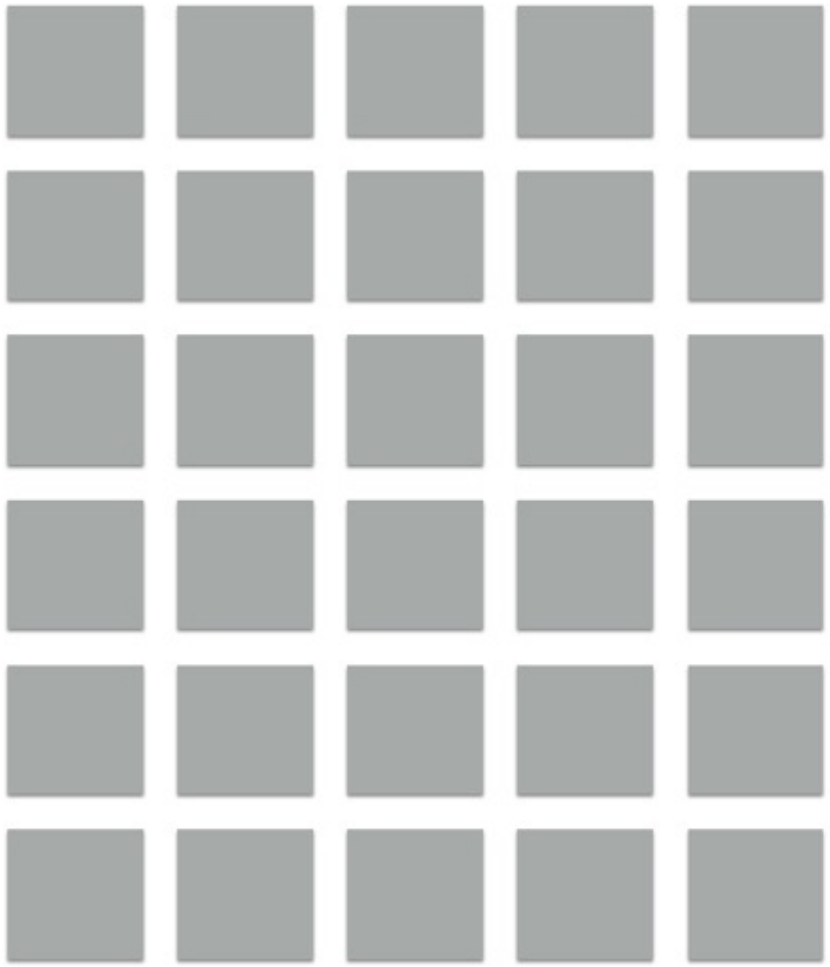
Existing problems

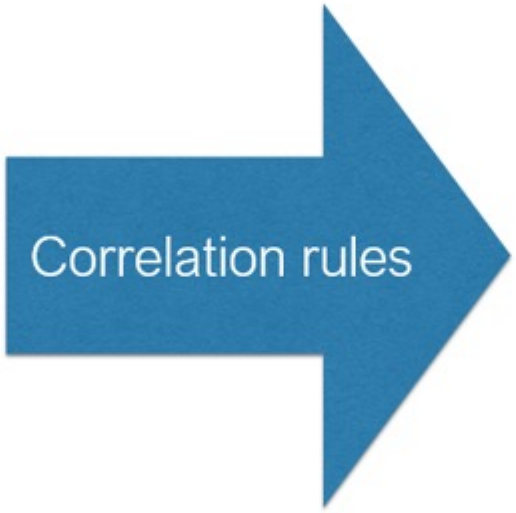


initMAX

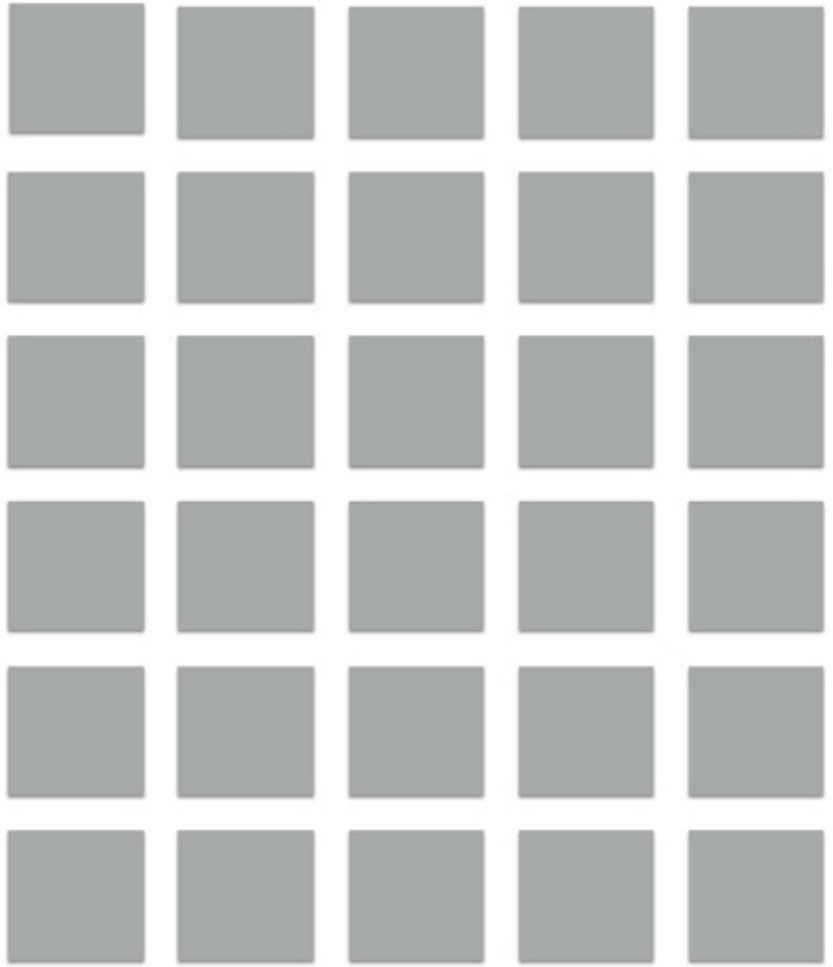
Event correlation

Existing problems





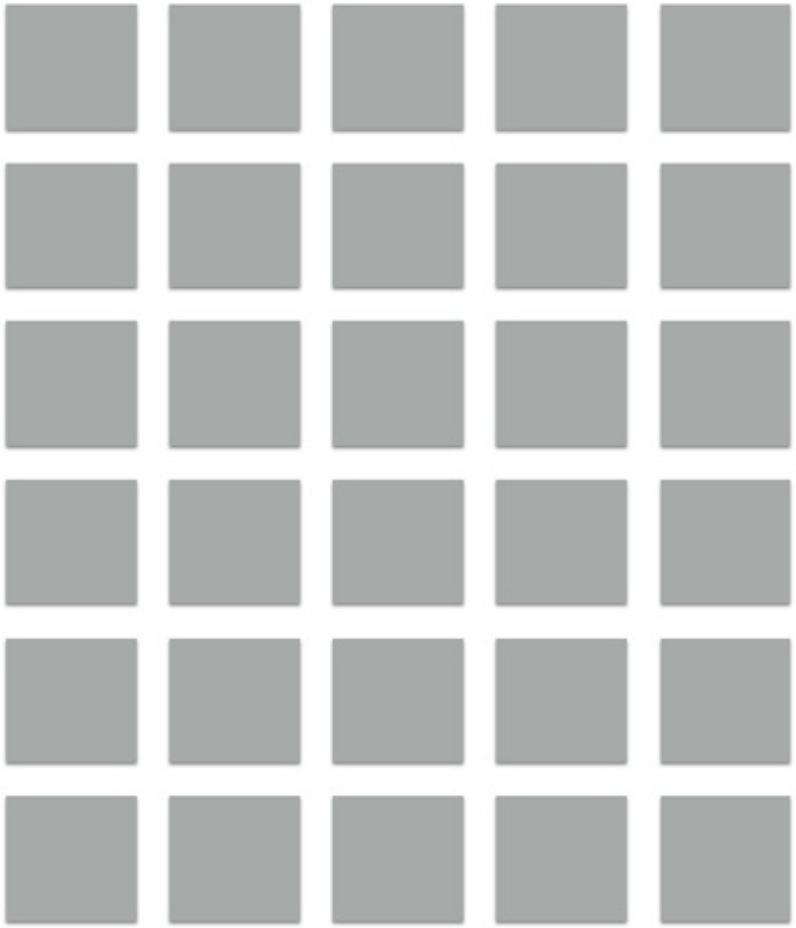
No correlation rules

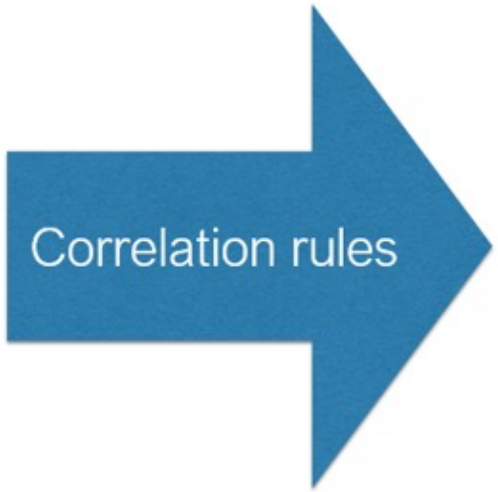


initMAX

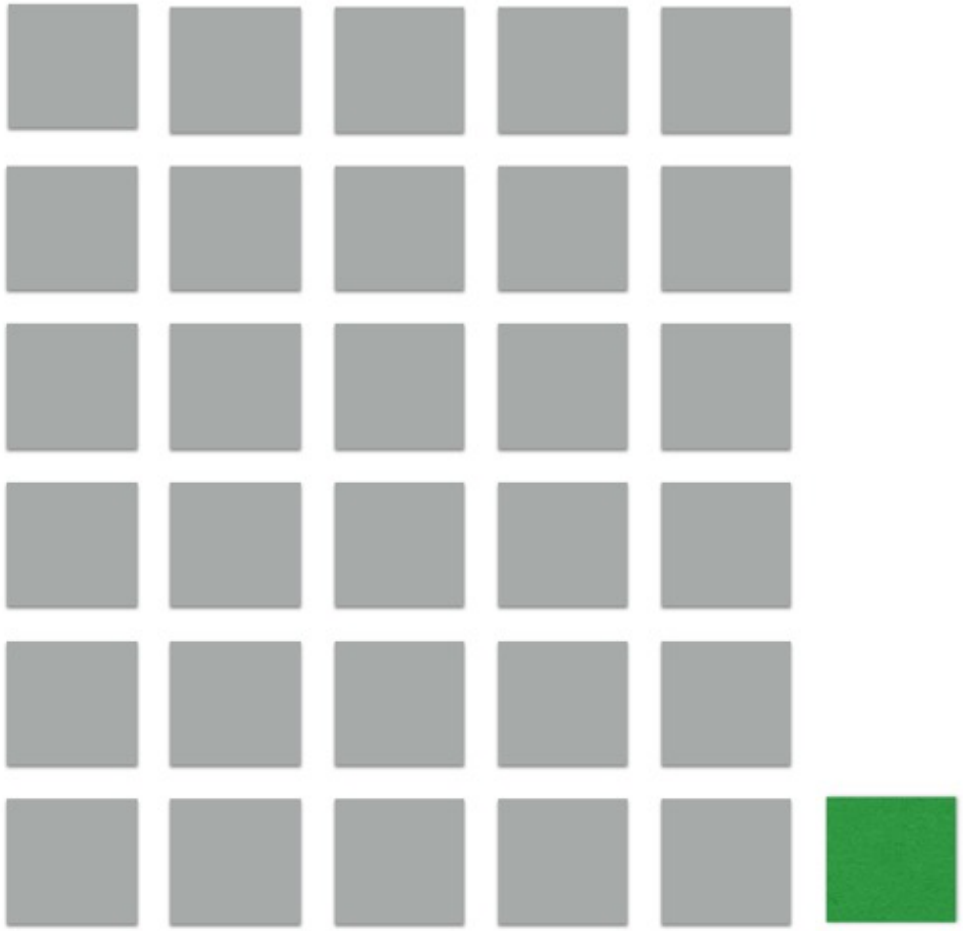
Event correlation

Existing problems





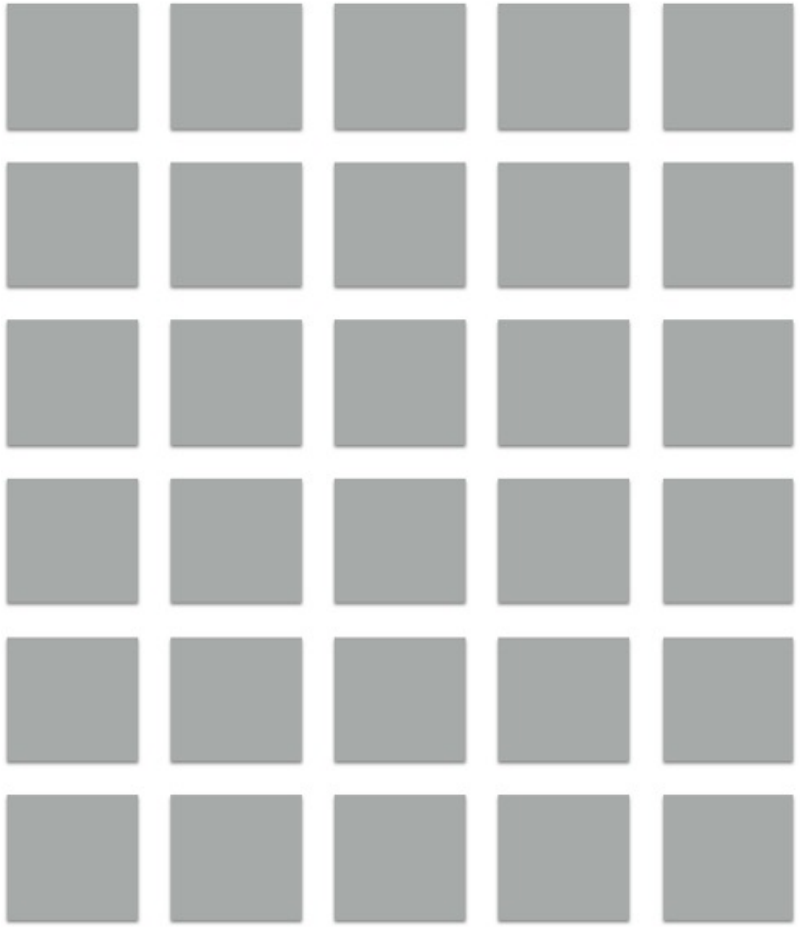
No correlation rules

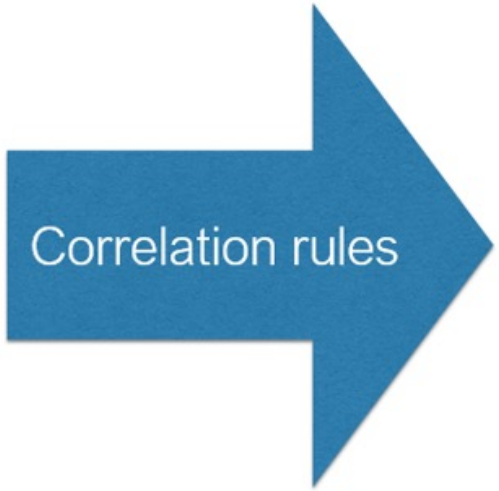


initMAX

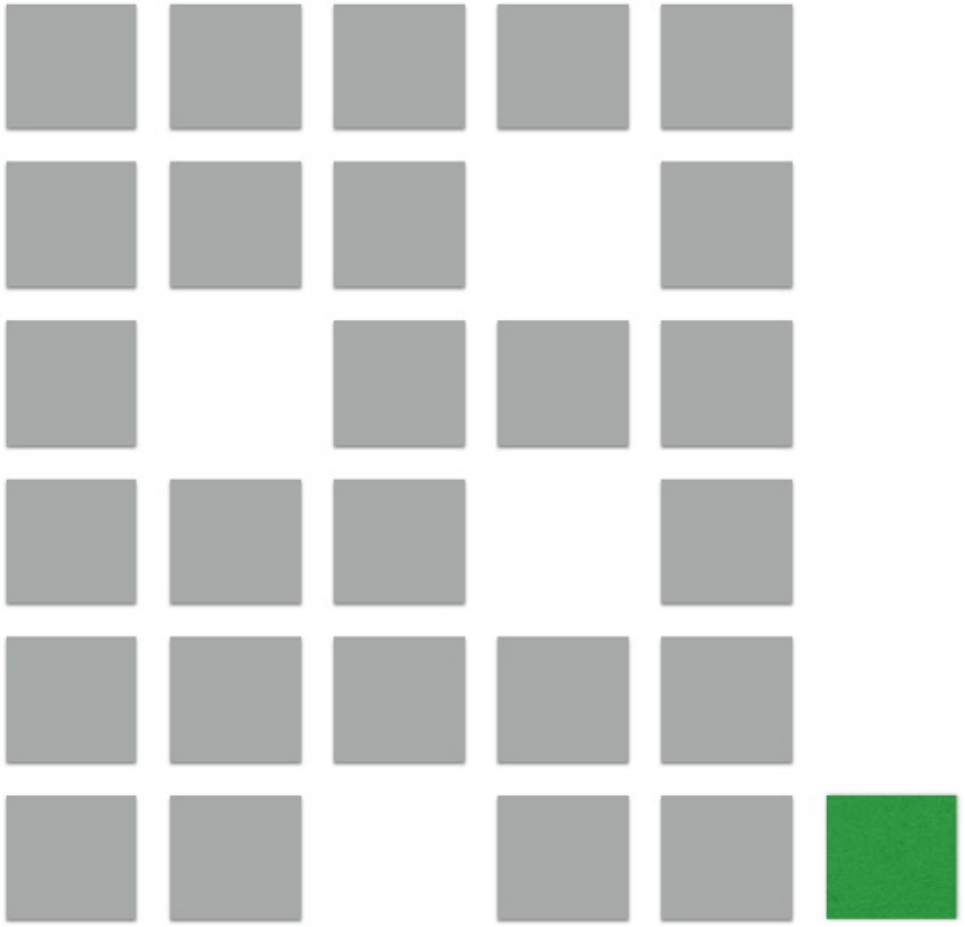
Event correlation

Existing problems





Correlation rules (close old)

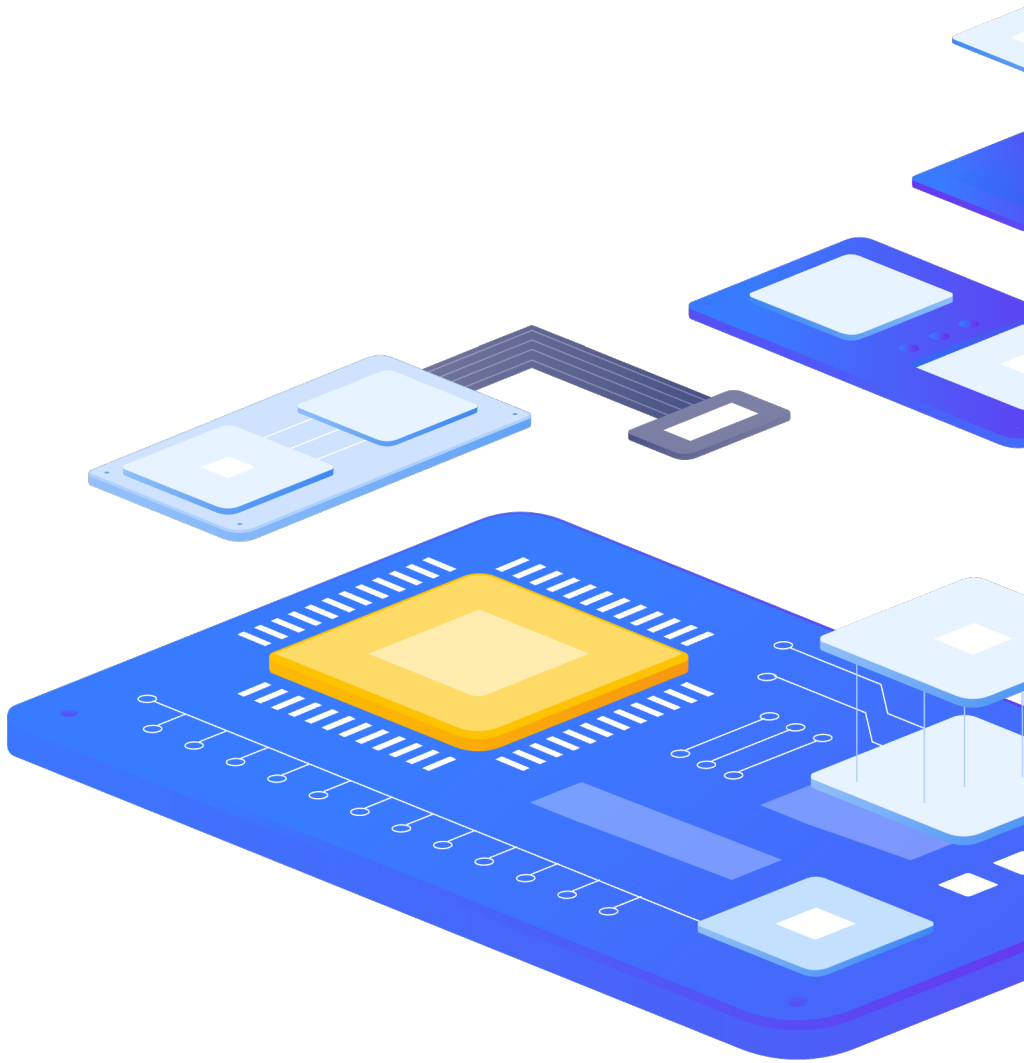


initMAX

ADVANCED PROBLEM DETECTION

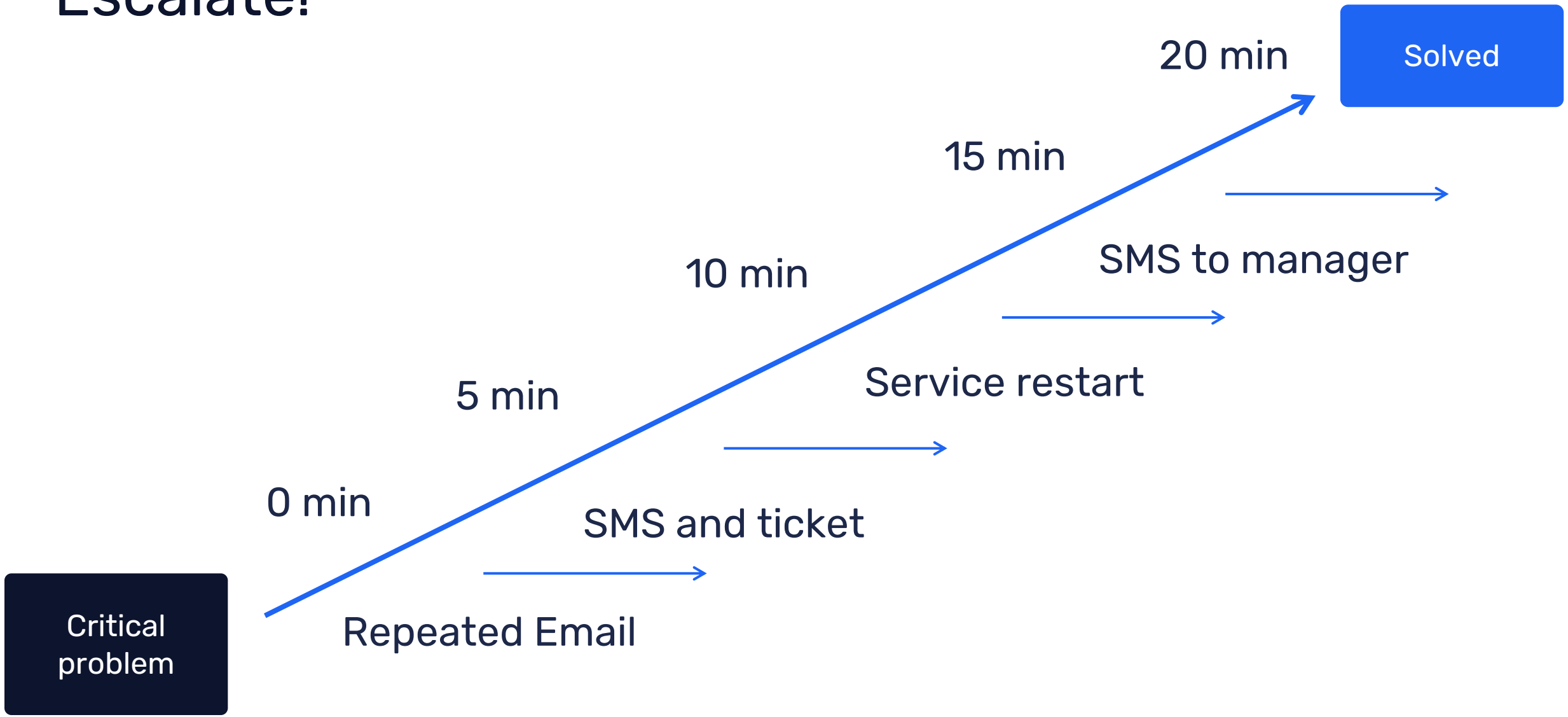
Escalate!

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



ADVANCED PROBLEM DETECTION

Escalate!



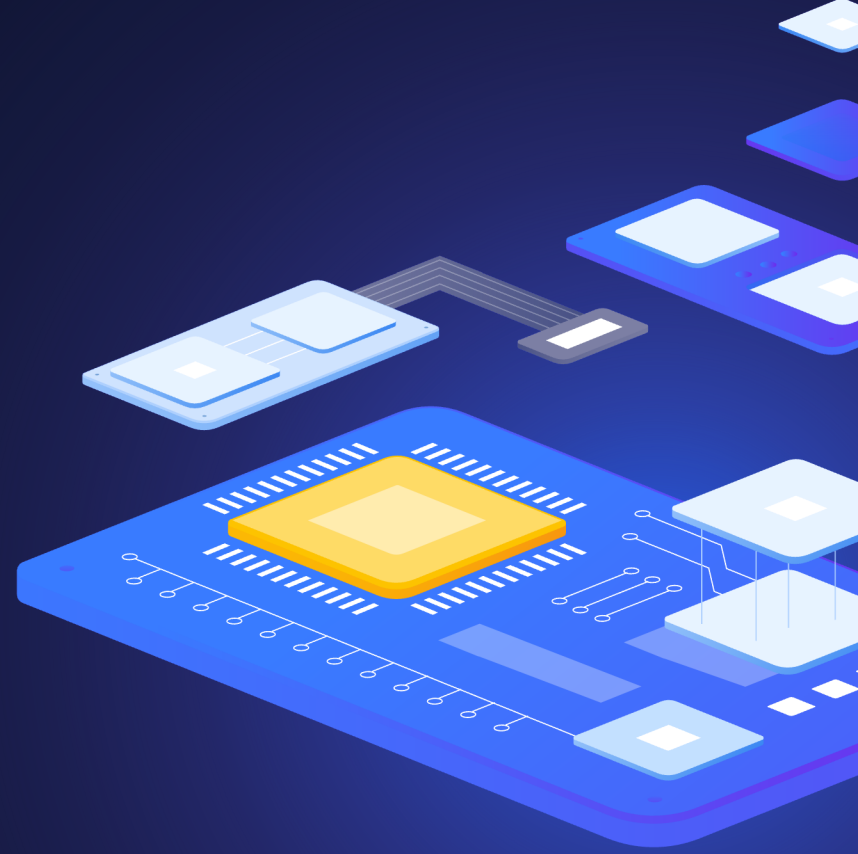
initMAX

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

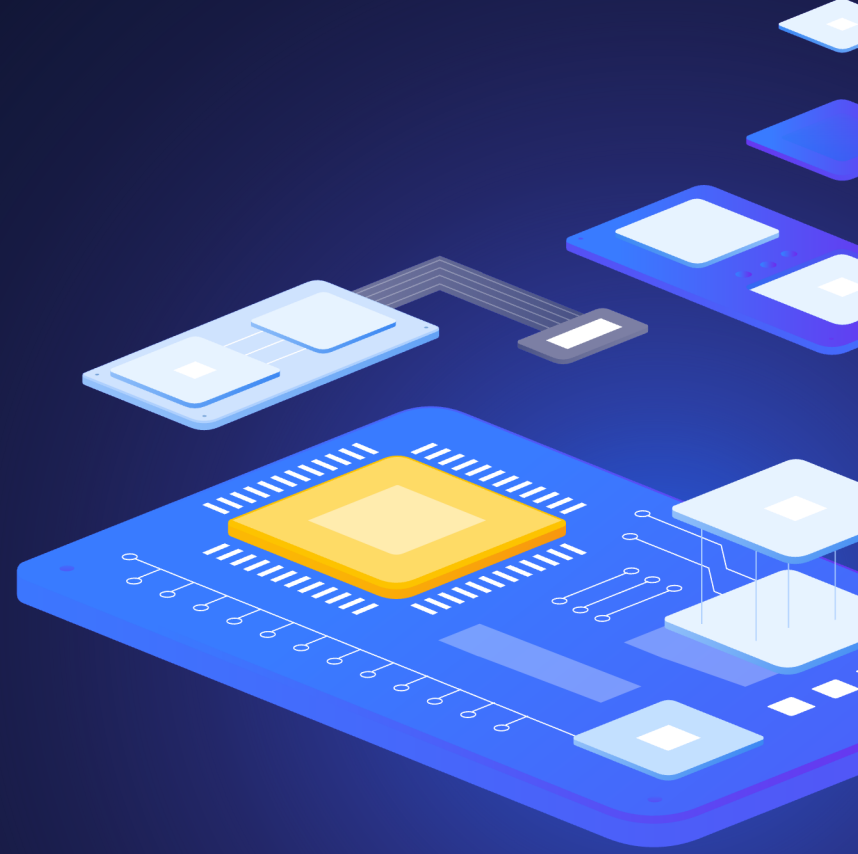
- Problem: Load of **Exchange** server increased by **24**% in **July** (**0.69**) comparing to **June** (**0.56**)

- 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

Cause and symptoms



ADVANCED PROBLEM DETECTION

Cause and symptom events

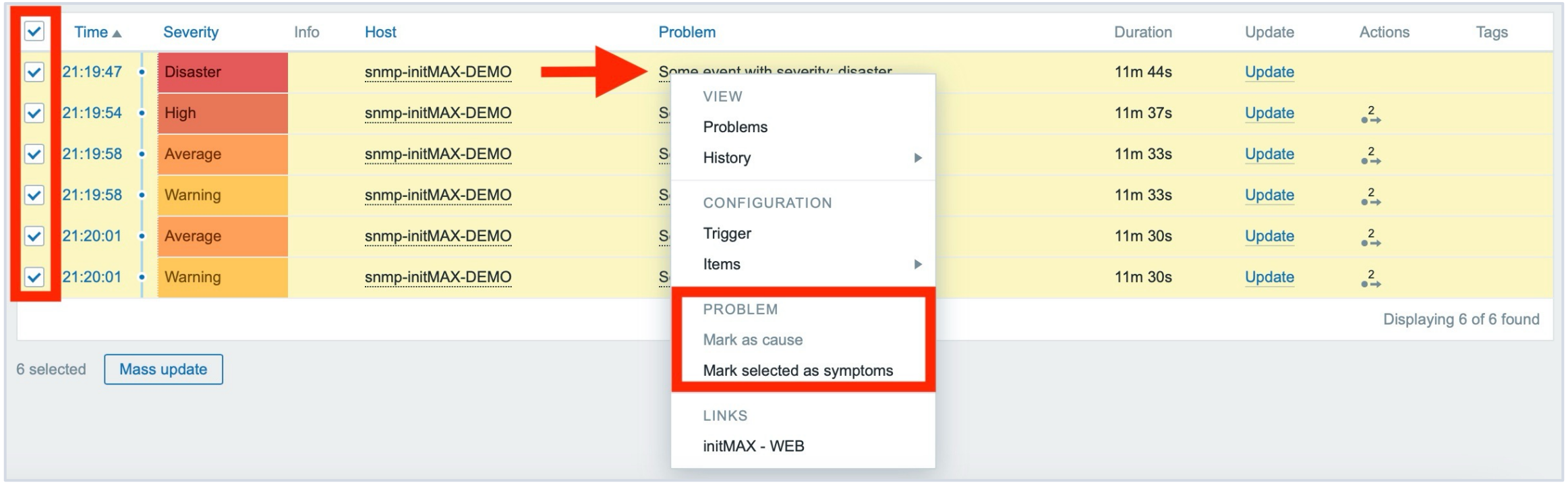
Zabbix 6.4 adds the ability to mark events as Cause or Symptom events. This allows Zabbix users to filter events in a way, where they can see only root cause problems, instead of being overwhelmed by symptom events

	Time ▲	Severity	Info	Host	Problem	Duration	Update	Actions
5	21:19:47	Disaster		snmp-initMAX-DEMO	Some event with severity: disaster	7m 46s	Update	
	21:19:54	High		snmp-initMAX-DEMO	Some event with severity: high	7m 39s	Update	1
	21:19:58	Average		snmp-initMAX-DEMO	Some event with severity: average	7m 35s	Update	1
	21:19:58	Warning		snmp-initMAX-DEMO	Some event with severity: warning	7m 35s	Update	1
	21:20:01	Average		snmp-initMAX-DEMO	Some event with severity: average	7m 32s	Update	1
	21:20:01	Warning		snmp-initMAX-DEMO	Some event with severity: warning	7m 32s	Update	1

ADVANCED PROBLEM DETECTION

Cause and symptom events

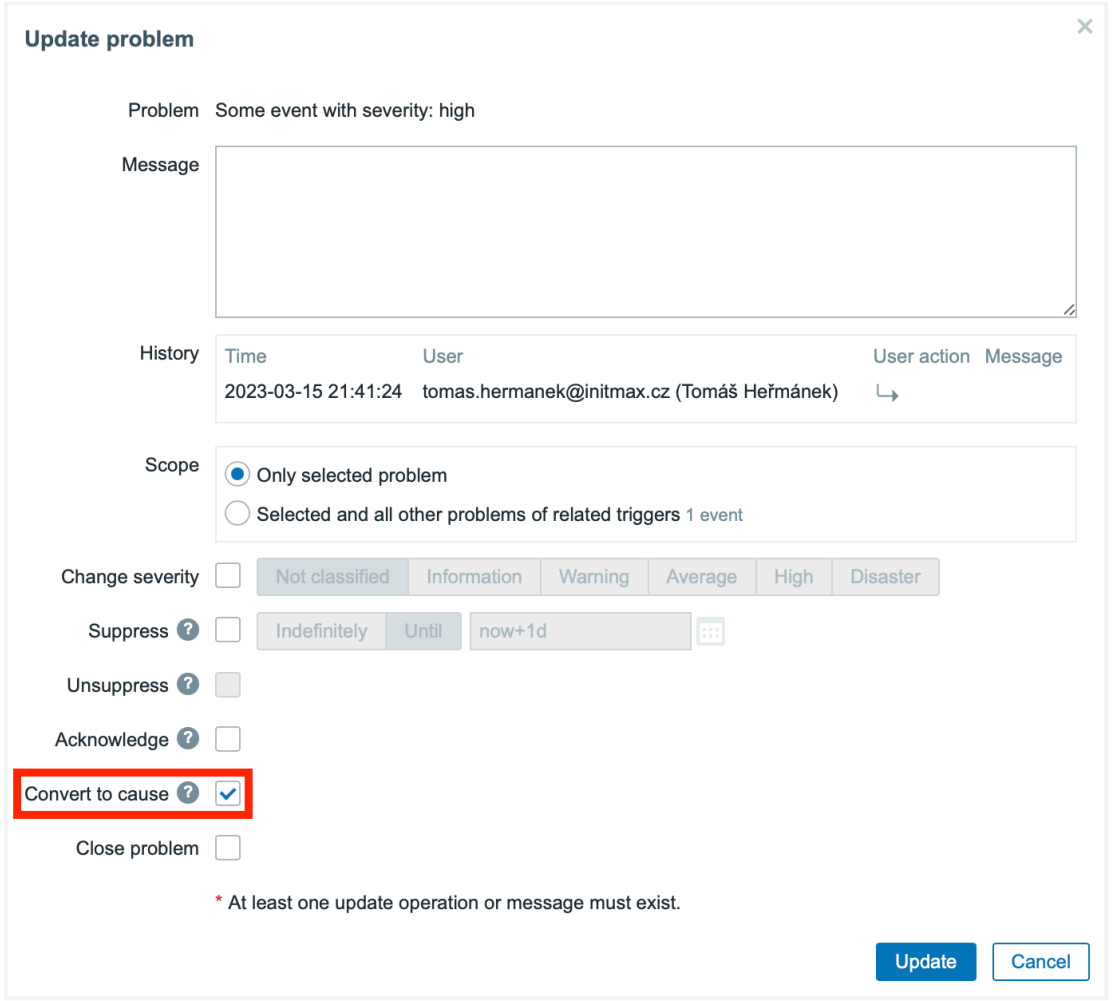
- Events can now be marked as cause or symptom events
- By default, all new problems are considered as cause events



ADVANCED PROBLEM DETECTION

Cause and symptom events

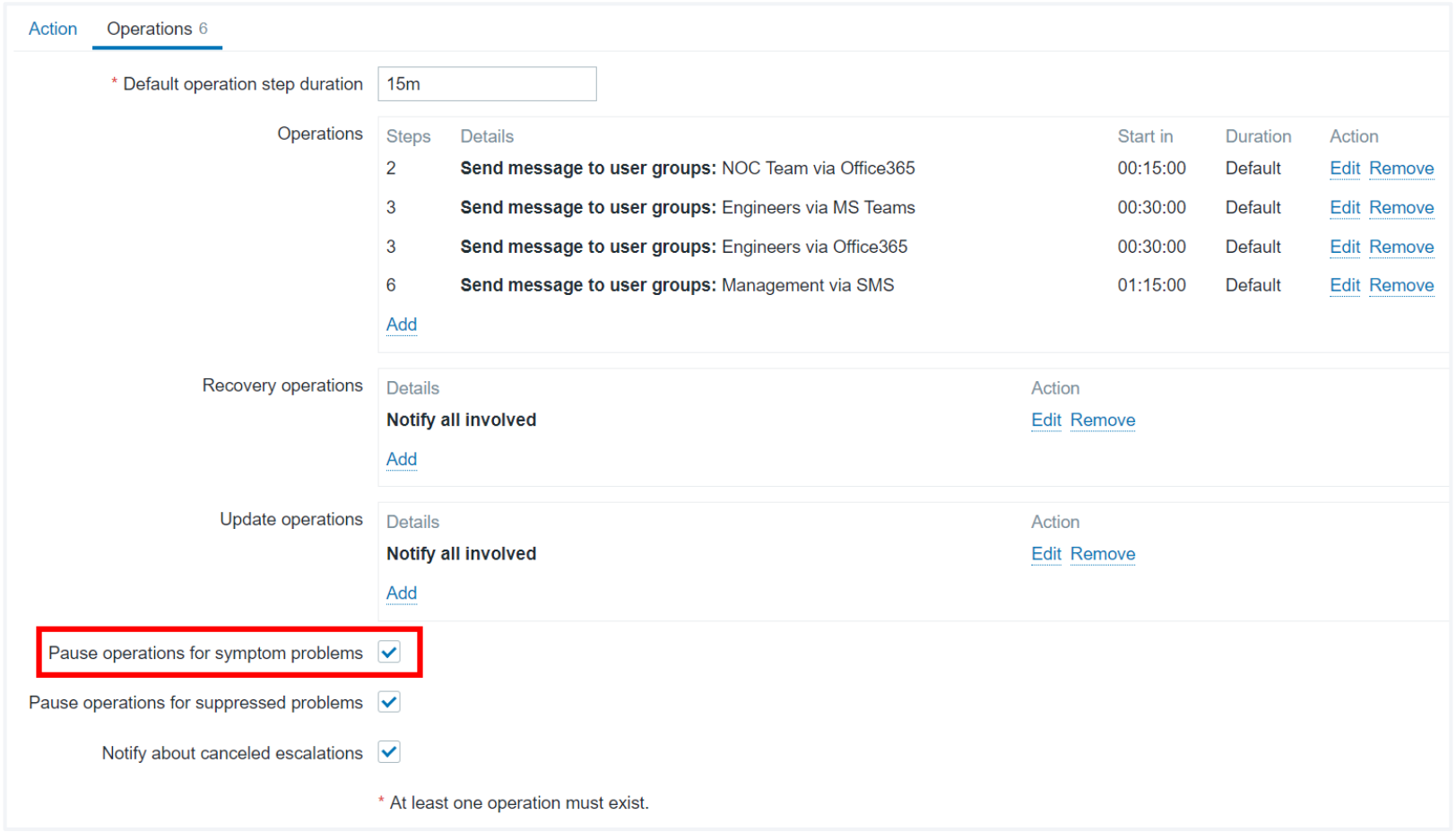
- Symptom events can be converted to cause events by pressing the update button in the problem list (previously – Ack button)



ADVANCED PROBLEM DETECTION

Symptom problems – actions

- It is possible to pause operations for symptom problems



ADVANCED PROBLEM DETECTION

Symptom problems – actions

Multiple new macros have been introduced to present cause events

- Cause event name - {EVENT.CAUSE.NAME}
- Cause event tags - {EVENT.CAUSE.TAGS}
- Cause event severity - {EVENT.CAUSE.SEVERITY
- Cause event status - {EVENT.CAUSE.STATUS}
- Cause event value - {EVENT.CAUSE.VALUE}
- More about new cause macros can be found in documentation https://www.zabbix.com/documentation/6.4/en/manual/appendix/macros/supported_by_location#cause-and-symptom-events

These macros can be used in

- Trigger-based notifications and commands
- Problem update notifications and commands
- Manual event action scripts

ADVANCED PROBLEM DETECTION

Cause and symptom events – API changes

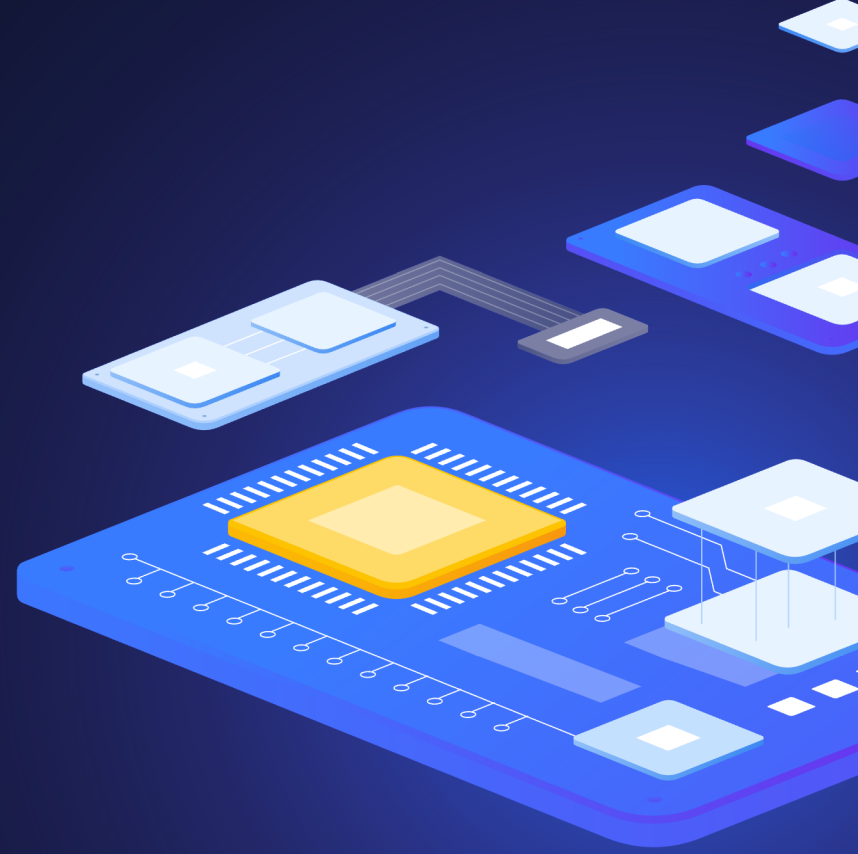
Multiple event related API calls now support filtering by cause and symptom events

- event.get and problem.get – new symptom parameter (true – symptom, false – cause)
- Cause event ID can also be returned in the request response:


```
{
    "jsonrpc": "2.0",
    "result": [
        {
            "eventid": "9695",
            "source": "0",
            "object": "0",
            "objectid": "13926",
            "clock": "1347970410",
            "value": "1",
            "acknowledged": "1",
            "ns": "413316245",
            "name": "MySQL is down",
            "severity": "5",
            "r_eventid": "0",
            "c_eventid": "0",
            "correlationid": "0",
            "userid": "0",
            "cause_eventid": "0",
            …
```

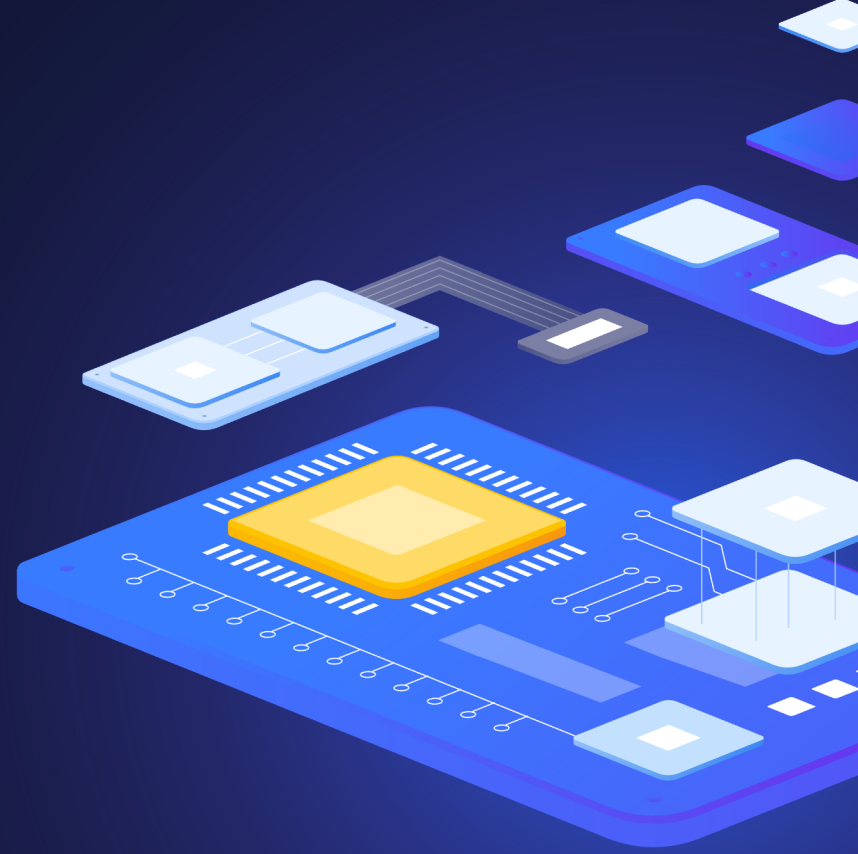
9

Demo



10

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