ZABBIX

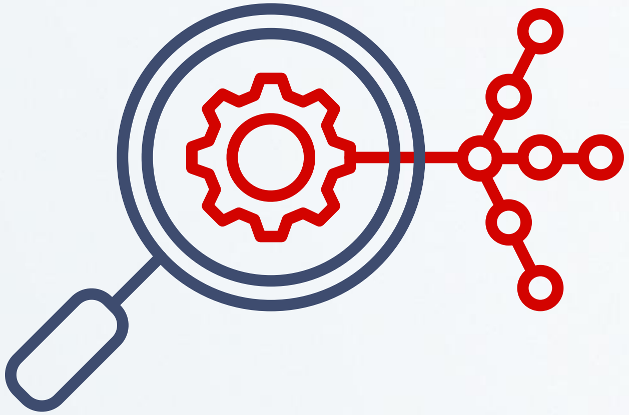
Detecting Root Cause Events with Zabbix

Aigars Kadikis

Technical Support Engineer & Zabbix Trainer

Why it’s good to get to root cause?

- Speed up problem-solving time
- More uptime
- Better reputation
- Avoid human mistakes
- Less noise, less headache



ZABBIX

Different methods of detecting root cause

- Trigger dependencies
- Triggers do not overlap
- Remove similar types of triggers
- Global event correlation
- Symptom and cause events

Trigger dependencies

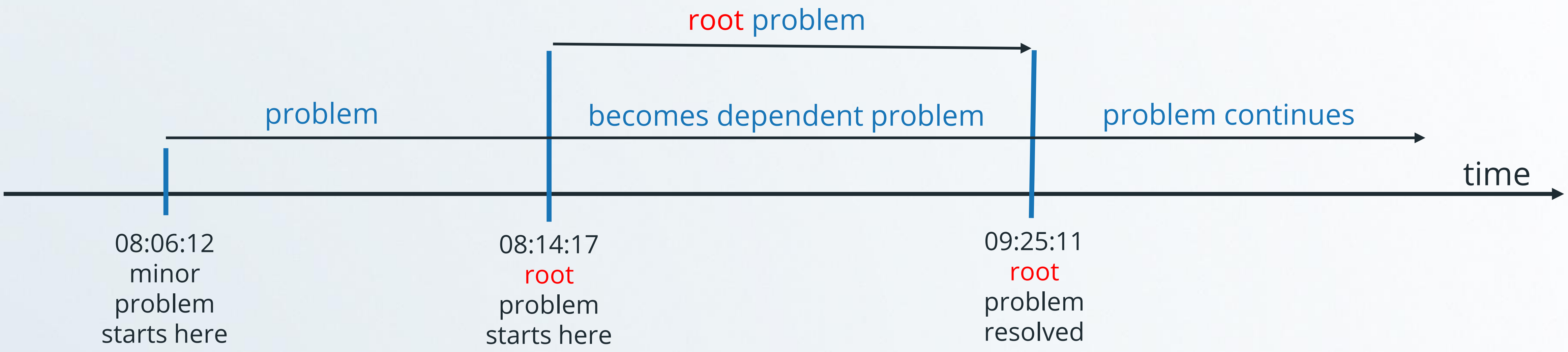
Pros

- Work with what’s already in templates
- Easy to use if all triggers belong to the same template

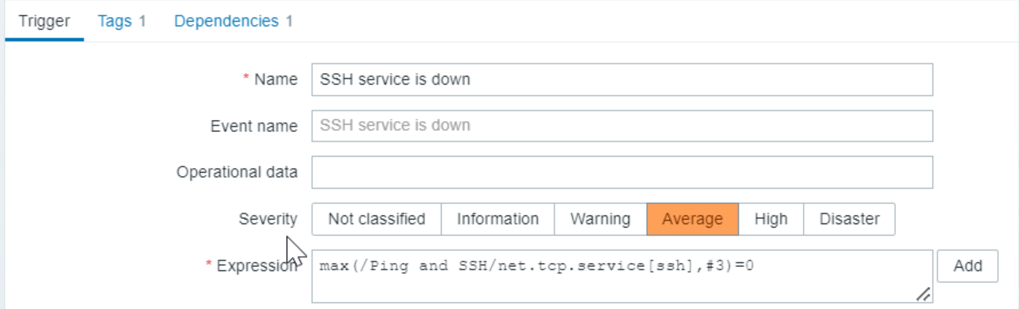
Cons

- Have to use the “History” tab to search for suppressed problems
- Have to use “flat” templates to save a dependency relation via “Template export”

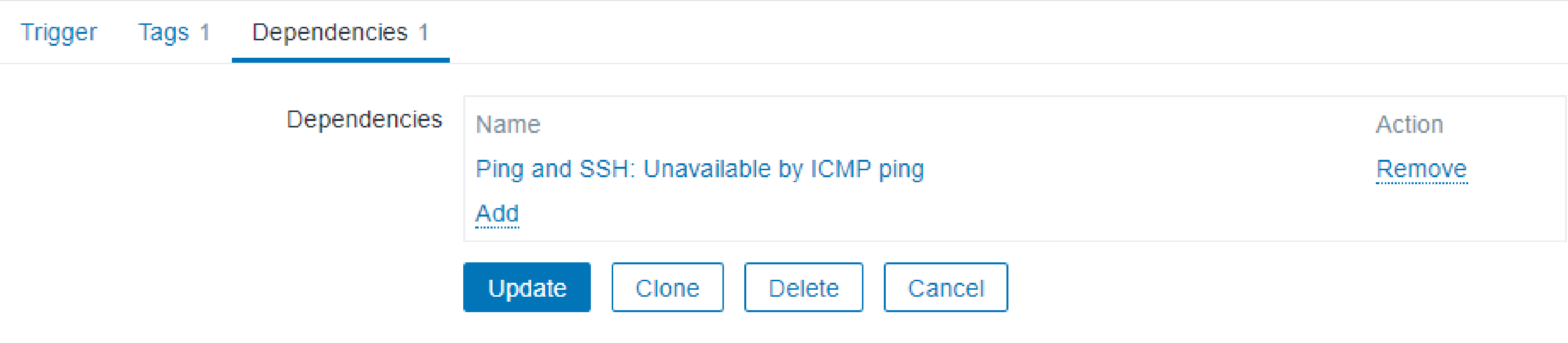
How trigger dependencies works?



Trigger dependencies in GUI

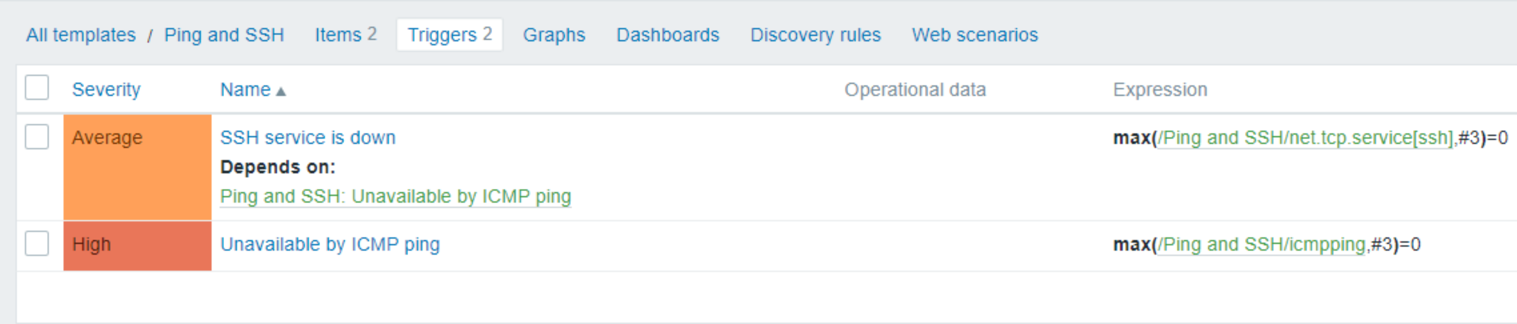


* Name	SSH service is down
Event name	SSH service is down
Operational data	
Severity	Not classified Information Warning [✓ Average] High Disaster
* Expression	max(/Ping and SSH/net.tcp.service[ssh],#3)=0

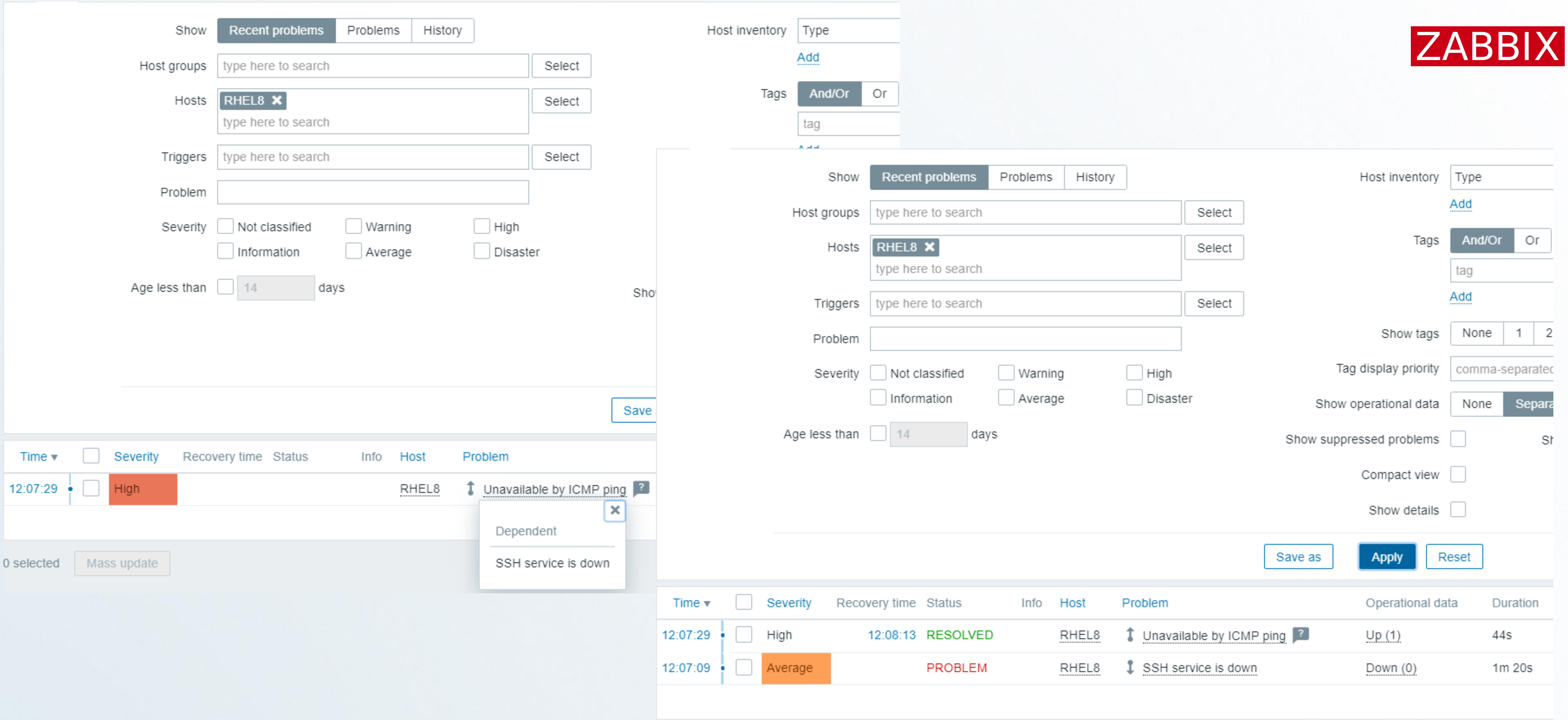


Dependencies

Name	Action
Ping and SSH: Unavailable by ICMP ping	Remove



□	Severity	Name ▲	Operational data	Expression
□	Average	SSH service is down **Depends on:** Ping and SSH: Unavailable by ICMP ping		**max(**/Ping and SSH/net.tcp.service[ssh],#3)=0
□	High	Unavailable by ICMP ping		**max(**/Ping and SSH/icmpping,#3)=0



Show: Recent problems | Problems | History

Host groups: type here to search Select

Hosts: RHEL8 ✕ type here to search Select

Triggers: type here to search Select

Problem:

Severity: □ Not classified □ Warning □ High □ Information □ Average □ Disaster

Age less than □ 14 days

Host inventory: Type Add

Tags: And/Or | Or tag Add

Save

Time ▾	□	Severity	Recovery time	Status	Info	Host	Problem
12:07:29	□	High				RHEL8	Unavailable by ICMP ping

Dependent

SSH service is down

0 selected Mass update

Show: Recent problems | Problems | History

Host groups: type here to search Select

Hosts: RHEL8 ✕ type here to search Select

Triggers: type here to search Select

Problem:

Severity: □ Not classified □ Warning □ High □ Information □ Average □ Disaster

Age less than □ 14 days

Host inventory: Type Add

Tags: And/Or | Or tag Add

Show tags: None | 1 | 2

Tag display priority: comma-separated

Show operational data: None | Separa

Show suppressed problems □

Compact view □

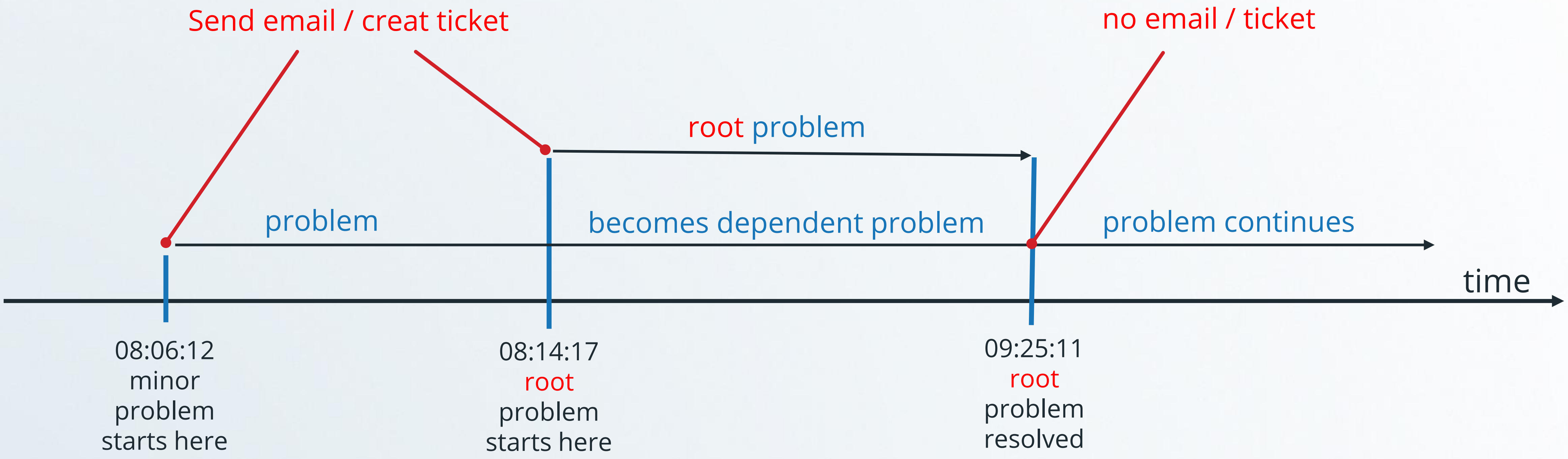
Show details □

Save as Apply Reset

Time ▾	□	Severity	Recovery time	Status	Info	Host	Problem	Operational data	Duration
12:07:29	□	High	12:08:13	RESOLVED		RHEL8	Unavailable by ICMP ping	Up (1)	44s
12:07:09	□	Average		PROBLEM		RHEL8	SSH service is down	Down (0)	1m 20s

If root cause is solved but SSH service is still down, then an extra email will not come because duration continues.

How trigger dependencies works?


Send email / creat ticket
no email / ticket
root problem
problem
becomes dependent problem
problem continues
time
08:06:12 minor problem starts here
08:14:17 root problem starts here
09:25:11 root problem resolved

ZABBIX

Triggers do not overlap

Use case 1:

- Different teams. Primary using emails/tickets to react

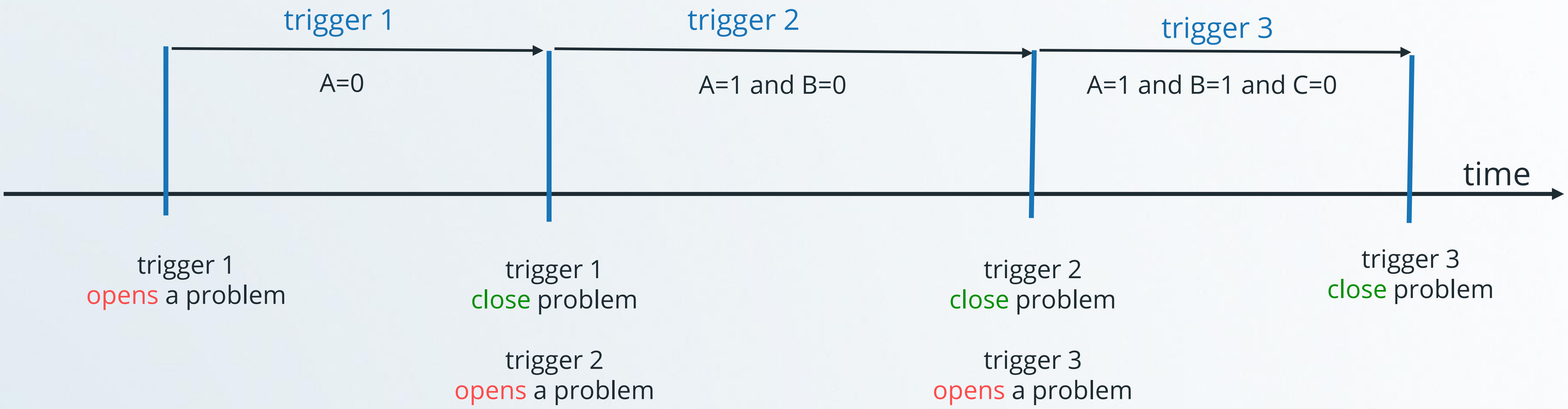
Use case 2:

- Doing a lot of agentless checks. Not using agents at all

Cons

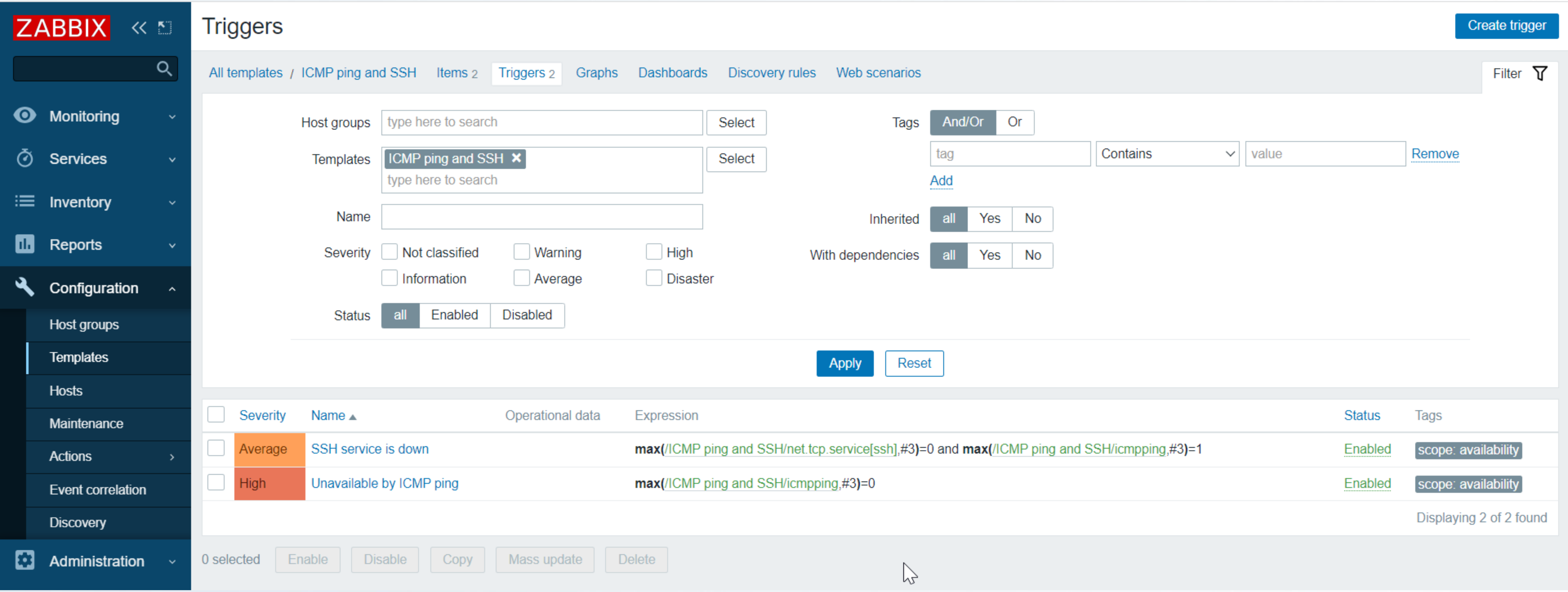
- More energy to implement
- Fine to use if only 2 or 3 essential items
- Will consume a little more CPU on calculation VS trigger dependencies

Triggers do not overlap



A trigger title works like a summary - what is the most important problem of this host right now?

Triggers do not overlap



Triggers

Host groups: type here to search [Select]

Templates: ICMP ping and SSH ✕ type here to search [Select]

Name:

Severity: □ Not classified □ Warning □ High □ Information □ Average □ Disaster

Status: [✓ all] Enabled Disabled

Tags: [✓ And/Or] Or

tag | Contains | value | Remove

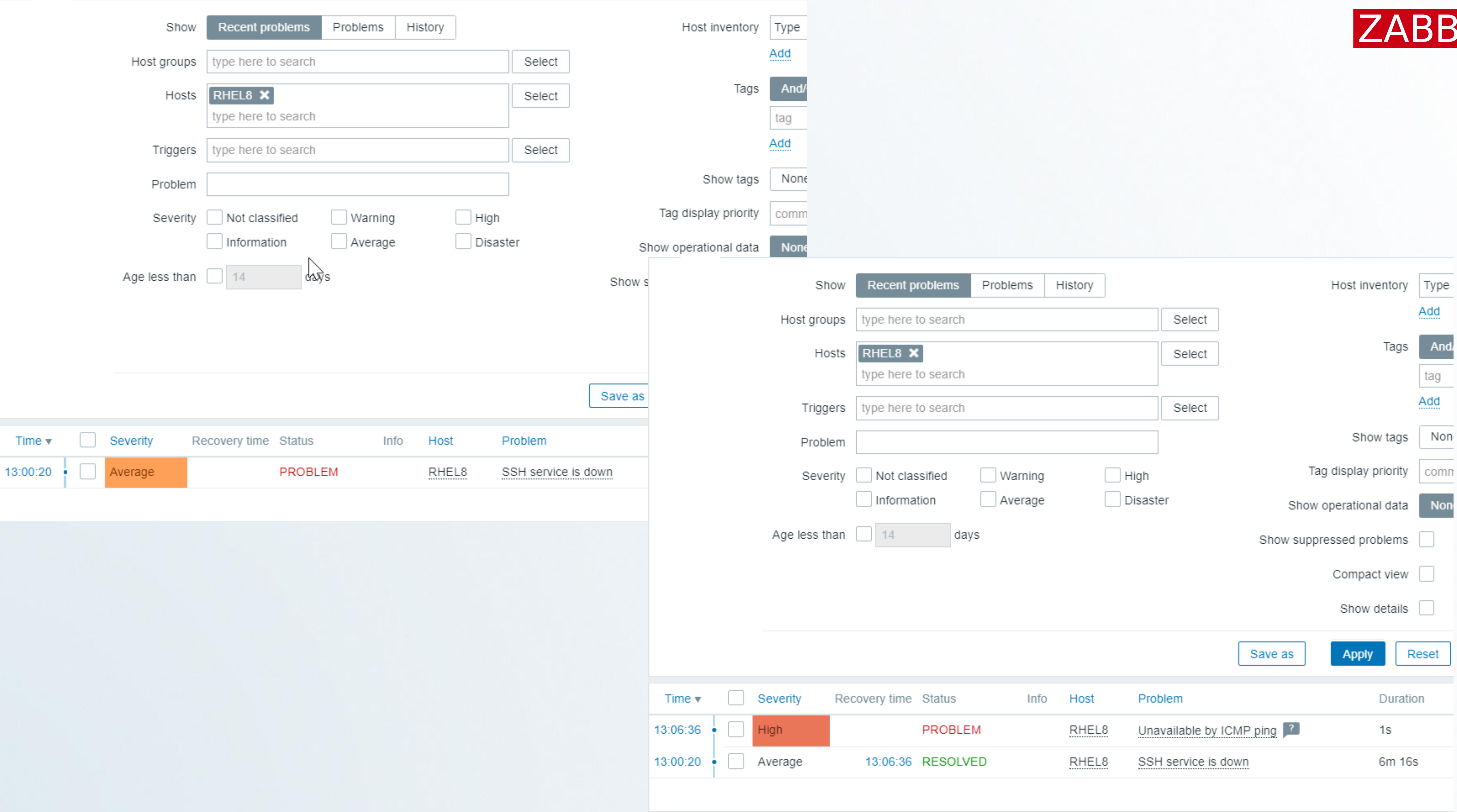
Add

Inherited: [✓ all] Yes No

With dependencies: [✓ all] Yes No

□	Severity	Name ▲	Operational data	Expression	Status	Tags
□	Average	SSH service is down		**max(**/ICMP ping and SSH/net.tcp.service[ssh],#3)=0 and **max(**/ICMP ping and SSH/icmpping,#3)=1	Enabled	scope: availability
□	High	Unavailable by ICMP ping		**max(**/ICMP ping and SSH/icmpping,#3)=0	Enabled	scope: availability

Displaying 2 of 2 found



Show: Recent problems | Problems | History
Host groups: type here to search — Select
Hosts: RHEL8 ✕ type here to search — Select
Triggers: type here to search — Select
Problem:
Severity: □ Not classified □ Warning □ High □ Information □ Average □ Disaster
Age less than □ 14 days

Host inventory: Type — Add
Tags: And/ — tag — Add
Show tags: None
Tag display priority: comm
Show operational data: None
Show s

Save as

Time ▾	□	Severity	Recovery time	Status	Info	Host	Problem
13:00:20	□	Average		PROBLEM		RHEL8	SSH service is down

Show: Recent problems | Problems | History
Host groups: type here to search — Select
Hosts: RHEL8 ✕ type here to search — Select
Triggers: type here to search — Select
Problem:
Severity: □ Not classified □ Warning □ High □ Information □ Average □ Disaster
Age less than □ 14 days

Host inventory: Type — Add
Tags: And/ — tag — Add
Show tags: Non
Tag display priority: comm
Show operational data: Non
Show suppressed problems □
Compact view □
Show details □

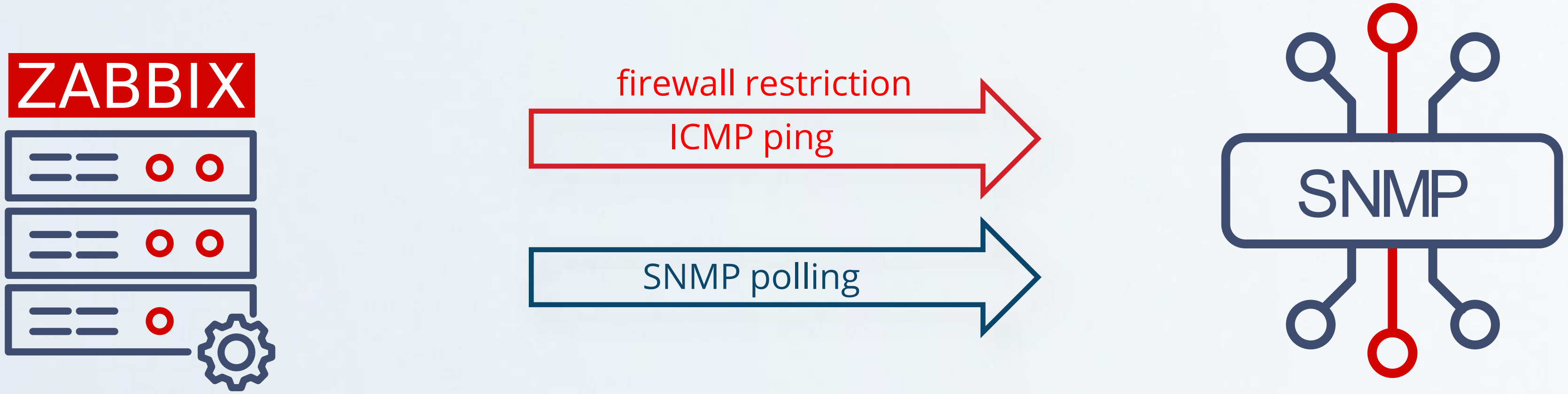
Save as | Apply | Reset

Time ▾	□	Severity	Recovery time	Status	Info	Host	Problem	Duration
13:06:36	□	High		PROBLEM		RHEL8	Unavailable by ICMP ping ?	1s
13:00:20	□	Average	13:06:36	RESOLVED		RHEL8	SSH service is down	6m 16s

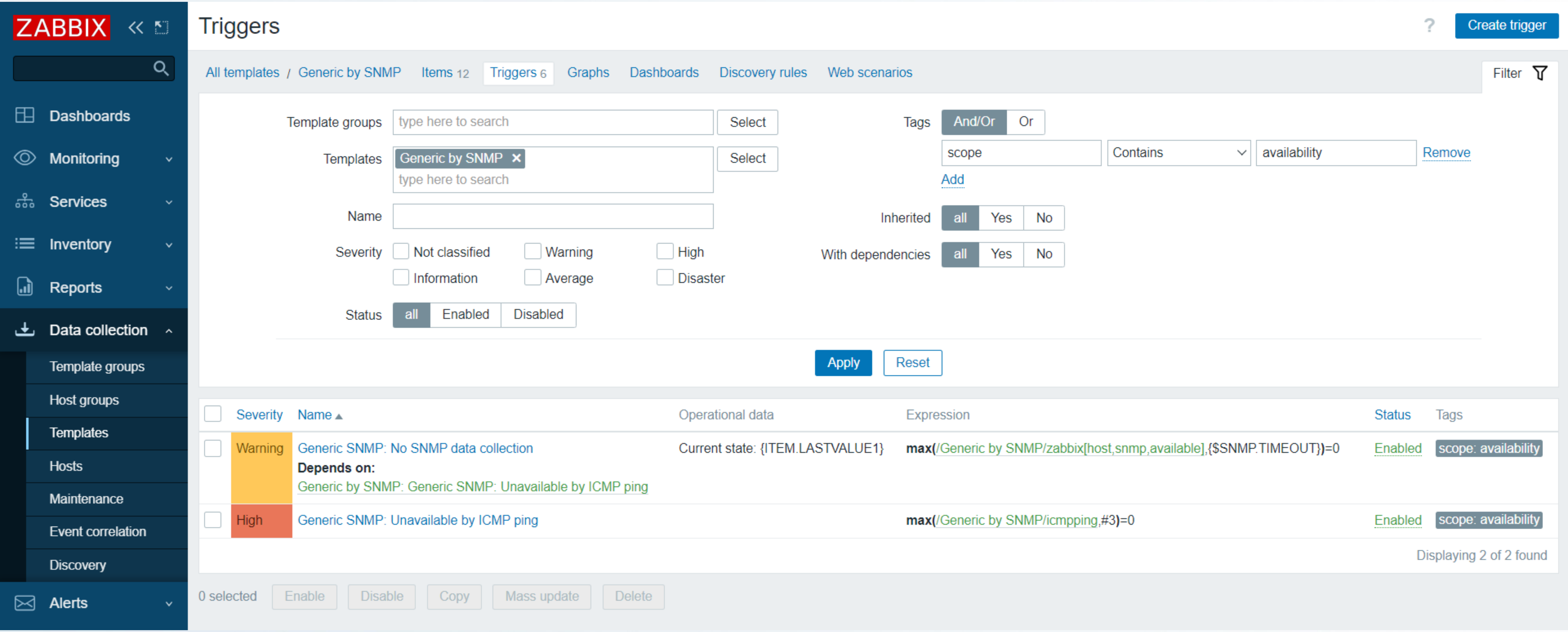
Remove similar type of trigger

«SNMP availability» VS «ICMP ping»

- When UDP 161 is not reachable, that is enough indication that devices have disappeared from network
- Sometimes ping probes are closed in firewall
- If the SNMP channel is not available, then we are not collecting health anymore



Remove similar type of trigger



Triggers

Template groups: type here to search

Templates: Generic by SNMP ✕

Name:

Severity: □ Not classified □ Warning □ High □ Information □ Average □ Disaster

Status: [✓ all] Enabled Disabled

Tags: [✓ And/Or] Or

scope | Contains | availability

Inherited: [✓ all] Yes No

With dependencies: [✓ all] Yes No

□	Severity	Name ▲	Operational data	Expression	Status	Tags
□	Warning	Generic SNMP: No SNMP data collection **Depends on:** Generic by SNMP: Generic SNMP: Unavailable by ICMP ping	Current state: {ITEM.LASTVALUE1}	**max(**/Generic by SNMP/zabbix[host,snmp,available],{$SNMP.TIMEOUT}**)**=0	Enabled	scope: availability
□	High	Generic SNMP: Unavailable by ICMP ping		**max(**/Generic by SNMP/icmpping,#3**)**=0	Enabled	scope: availability

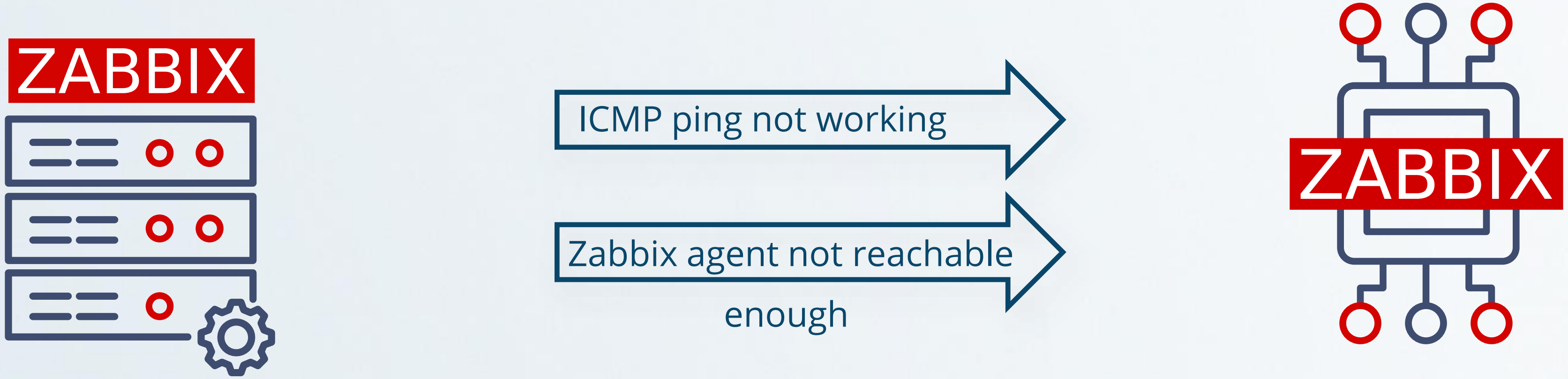
Displaying 2 of 2 found

ZABBIX

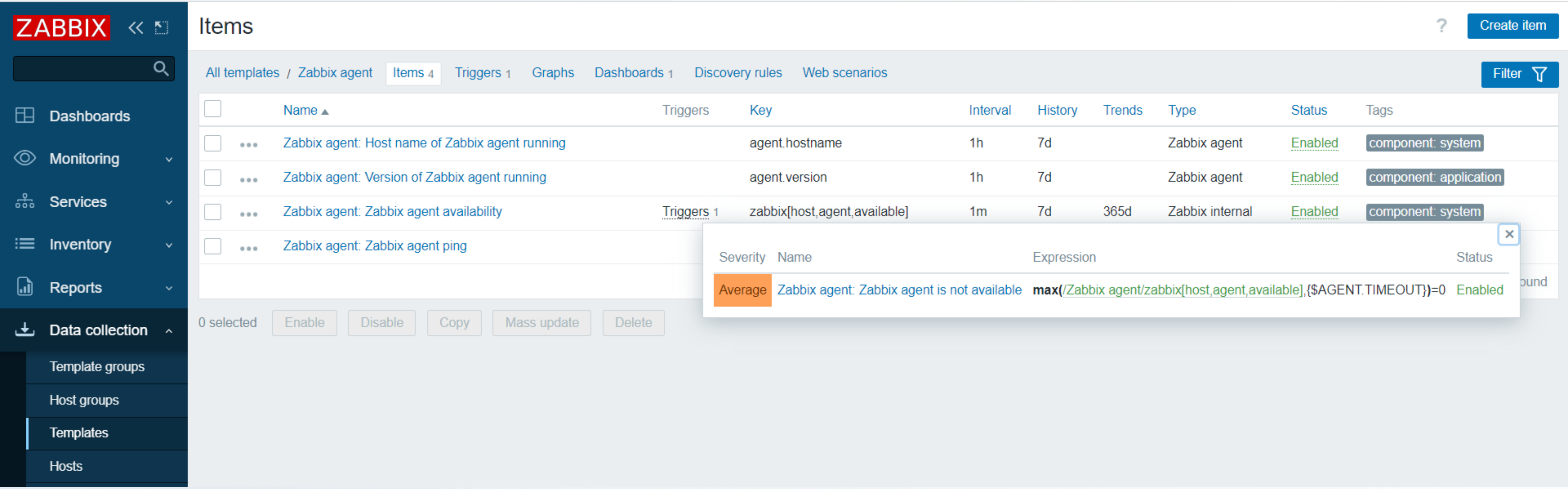
Remove similar type of triggers

«Agent ping» VS «ICMP ping»

- If we treat agent monitoring with a high-priority
  - ✓ Why use ICMP ping together with Zabbix agent ping?
  - ✓ Passive Agent ping better than active ping. Plus, we can use remote commands



Remove similar type of triggers



Items

☐		Name ▲	Triggers	Key	Interval	History	Trends	Type	Status	Tags
☐	•••	Zabbix agent: Host name of Zabbix agent running		agent.hostname	1h	7d		Zabbix agent	Enabled	component: system
☐	•••	Zabbix agent: Version of Zabbix agent running		agent.version	1h	7d		Zabbix agent	Enabled	component: application
☐	•••	Zabbix agent: Zabbix agent availability	Triggers 1	zabbix[host,agent,available]	1m	7d	365d	Zabbix internal	Enabled	component: system
☐	•••	Zabbix agent: Zabbix agent ping								

0 selected

Severity	Name	Expression	Status
Average	Zabbix agent: Zabbix agent is not available	max(/Zabbix agent/zabbix[host,agent,available],{$AGENT.TIMEOUT})=0	Enabled

If we treat Windows/Linux monitoring with high priority – it's critical when Zabbix agent is down

Global correlation

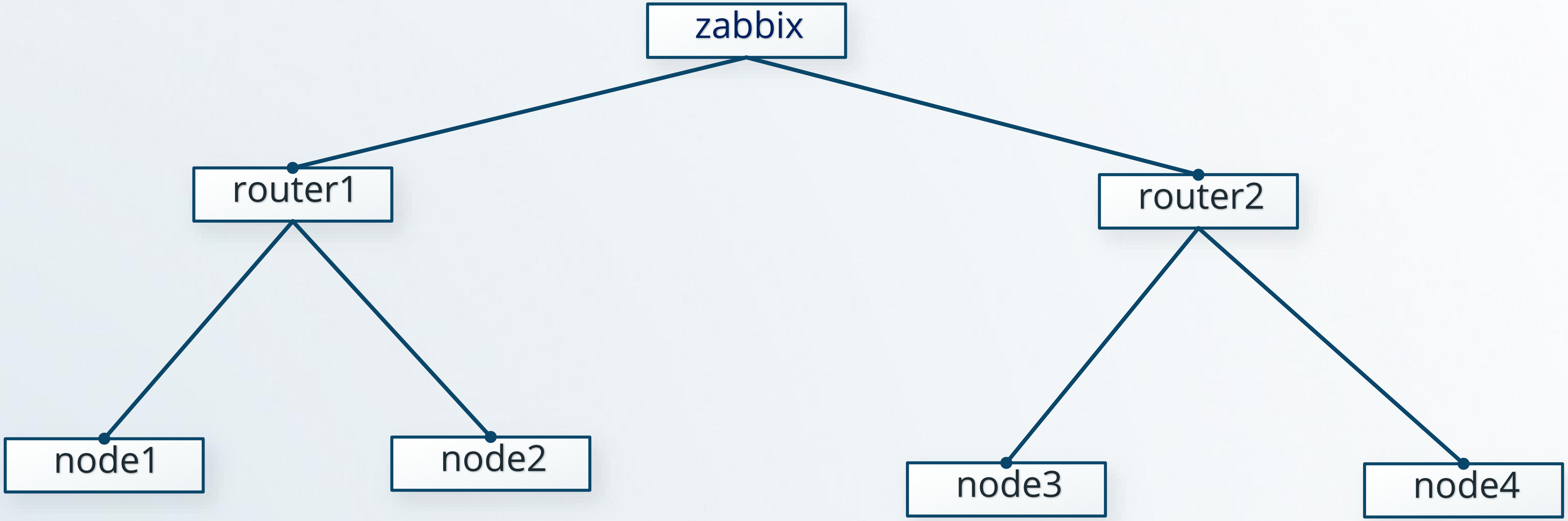
Use case:

- Device hierarchy. ISP situation
- Availability trigger is critical

Cons

- Will pile up database very fast - slow down GUI experience
- Will generate an unexpected CPU load
- Safer to use with a new deployment

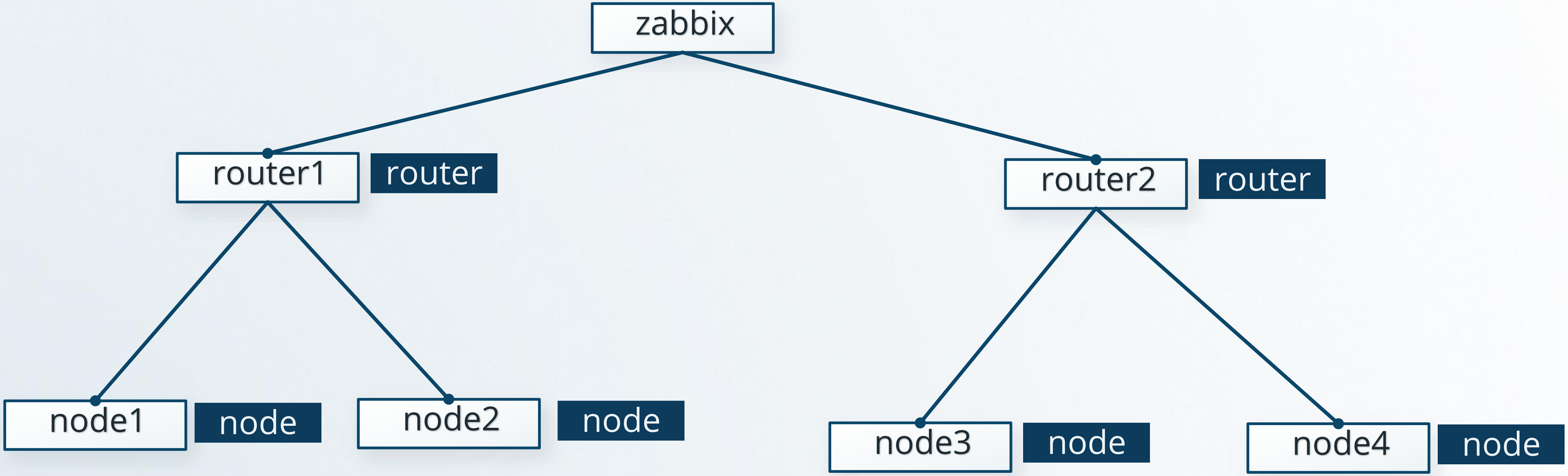
Global correlation - hierarchy with tag pair



Availability check

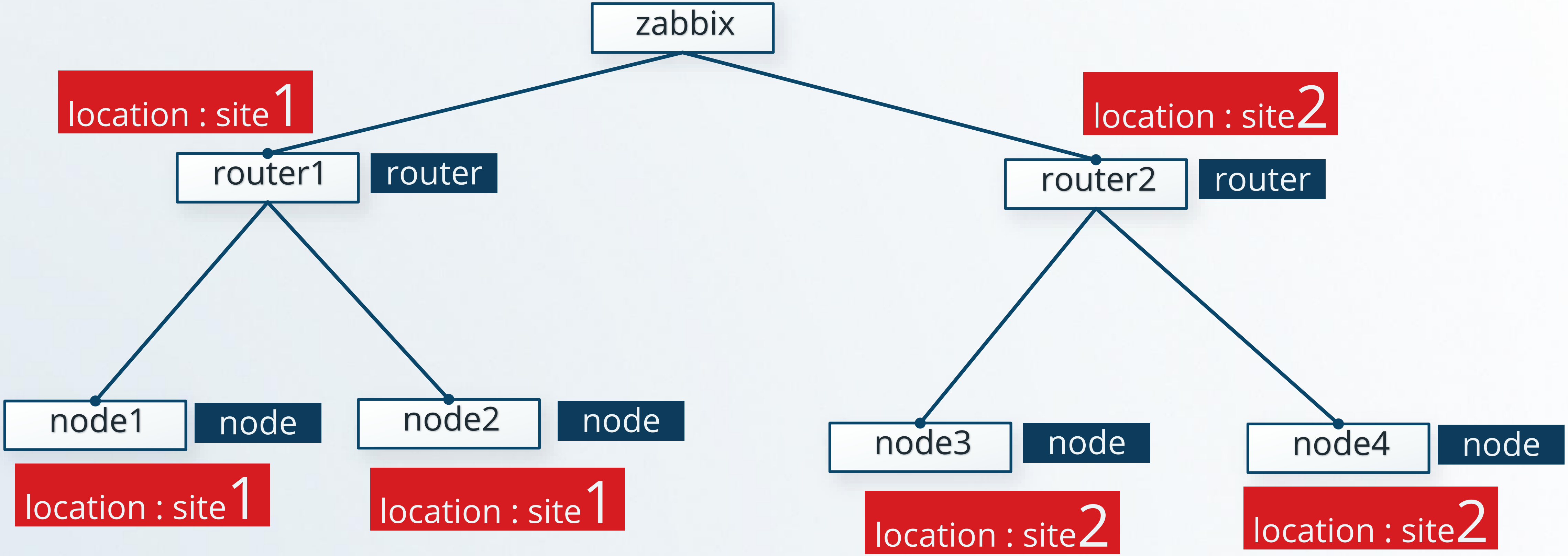
ZABBIX

Global correlation - hierarchy with tag pair



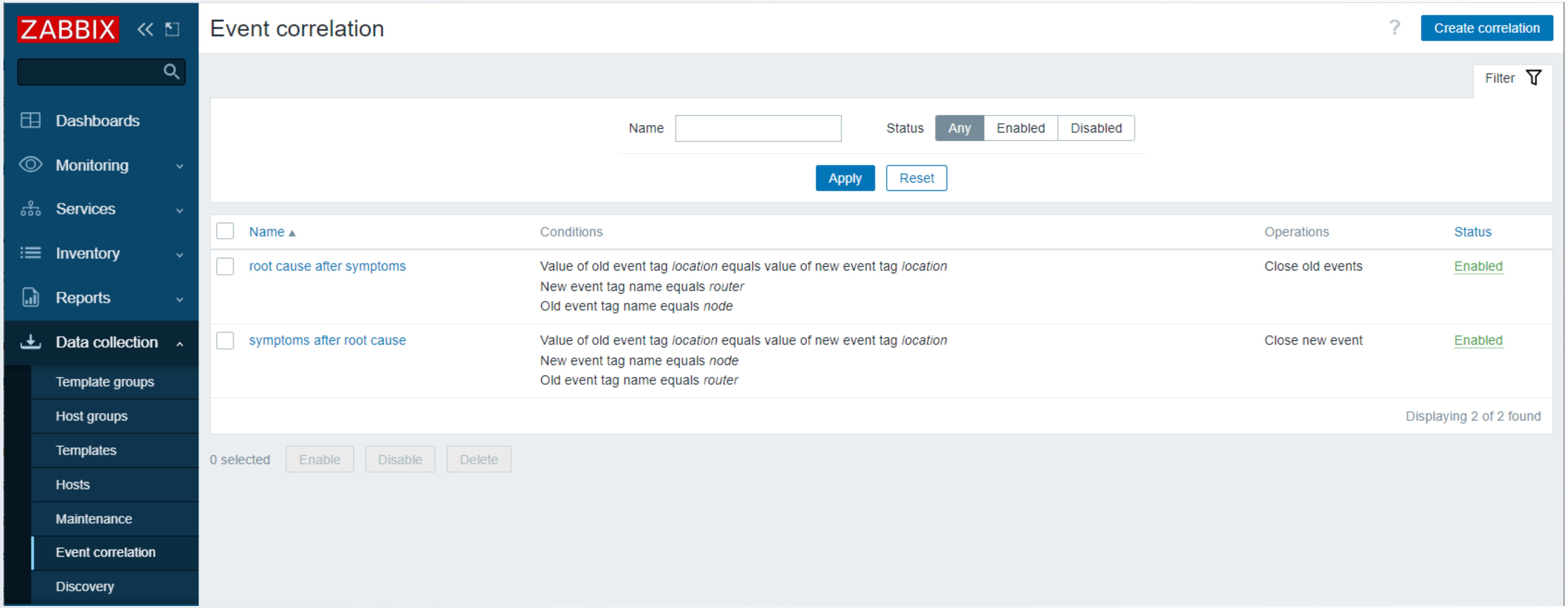
Create a tag without a value

Global correlation - hierarchy with tag pair



Create a tag «location» with a value. Map devices to location

Global correlation - hierarchy with tag pair



Event correlation

Name □ Status: [✓ Any] Enabled Disabled

□	Name ▲	Conditions	Operations	Status
□	root cause after symptoms	Value of old event tag *location* equals value of new event tag *location* New event tag name equals *router* Old event tag name equals *node*	Close old events	Enabled
□	symptoms after root cause	Value of old event tag *location* equals value of new event tag *location* New event tag name equals *node* Old event tag name equals *router*	Close new event	Enabled

Displaying 2 of 2 found

We do not need to hardcode the location value

ZABBIX

Symptom and cause events

Use case:

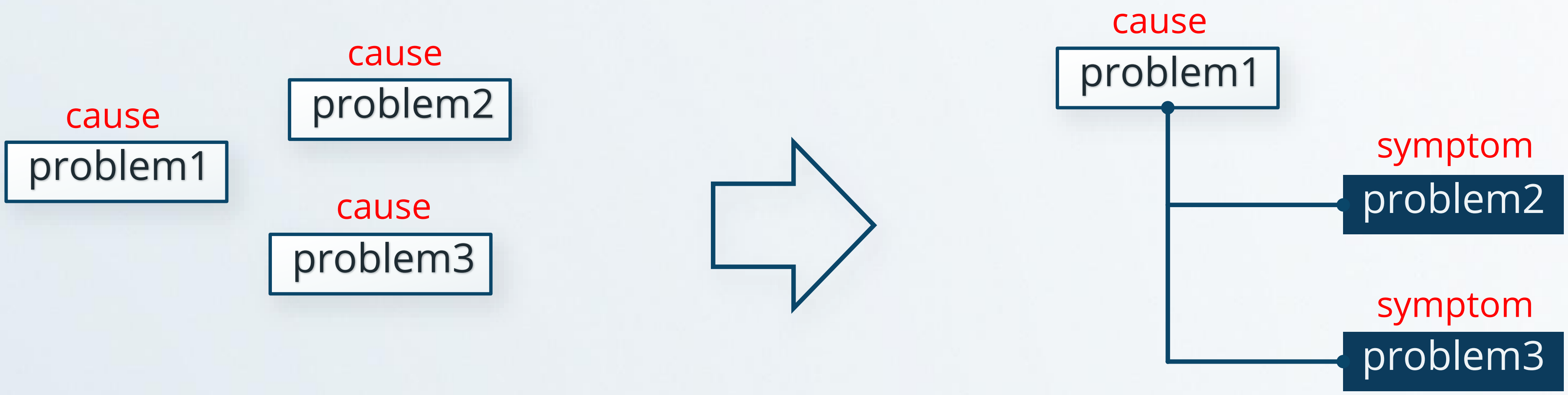
- Keep symptoms - evidence
- Event cascade too unique every time
- Monitoring at the beginning phase – just getting started
- Extra framework to work with outcome (events)

Cons

- Support only two levels
- Must redo the marking every time

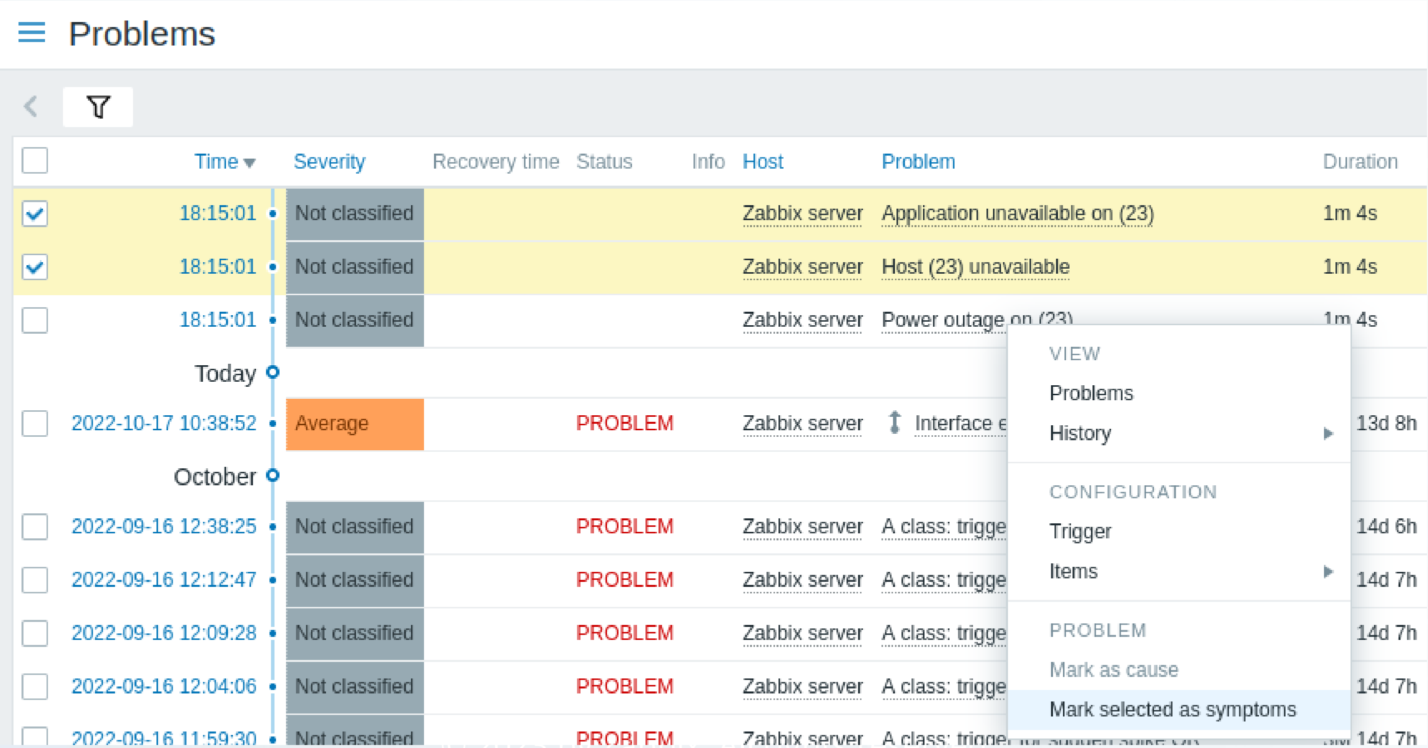
How symptom and cause events work?

- Manually reclassify specific problems as symptom problems of the cause problem
- Is it possible to re-make everything as cause and start all over



Symptom and cause events in GUI

1. Select 1 or multiple symptom events
2. Locate target/cause event and click on event title
3. Select «Mark selected as symptoms»



Problems

□	Time ▾	Severity	Recovery time	Status	Info	Host	Problem	Duration
☑	18:15:01	Not classified				Zabbix server	Application unavailable on (23)	1m 4s
☑	18:15:01	Not classified				Zabbix server	Host (23) unavailable	1m 4s
□	18:15:01	Not classified				Zabbix server	Power outage on (23)	1m 4s
	Today							
□	2022-10-17 10:38:52	Average		PROBLEM		Zabbix server	↥ Interface e	13d 8h
	October							
□	2022-09-16 12:38:25	Not classified		PROBLEM		Zabbix server	A class: trigge	14d 6h
□	2022-09-16 12:12:47	Not classified		PROBLEM		Zabbix server	A class: trigge	14d 7h
□	2022-09-16 12:09:28	Not classified		PROBLEM		Zabbix server	A class: trigge	14d 7h
□	2022-09-16 12:04:06	Not classified		PROBLEM		Zabbix server	A class: trigge	14d 7h
□	2022-09-16 11:59:30	Not classified		PROBLEM		Zabbix server	A class: trigger	14d 7h

ZABBIX

Thank you!

Aigars Kadikis

Technical Support Engineer & Zabbix Trainer