

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



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

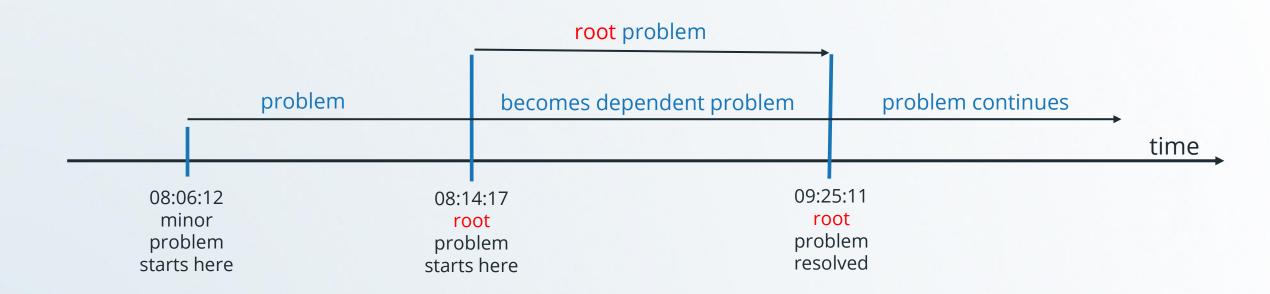
Cons

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

Tags 1	Dependencies 1		
	* Name	SSH service is down	
	Event name	SSH service is down	
	Operational data		
	Severity	Not classified Information Warning Average High Disaster	
	* Expression	<pre>max(/Ping and SSH/net.tcp.service[ssh],#3)=0</pre>	Add
	Tags 1	* Name Event name Operational data Severity	Name SSH service is down Event name SSH service is down Operational data Severity Not classified Information Warning Average High Disaster

Trigger	Tags 1	Dependencies 1		
		Dependencies	Name Ping and SSH: Unavailable by ICMP ping Add	Action Remove
			Update Clone Delete Cancel	

All templates / Ping and SSH Items 2 Triggers 2 Graphs Dashboards Discovery rules Web scenarios

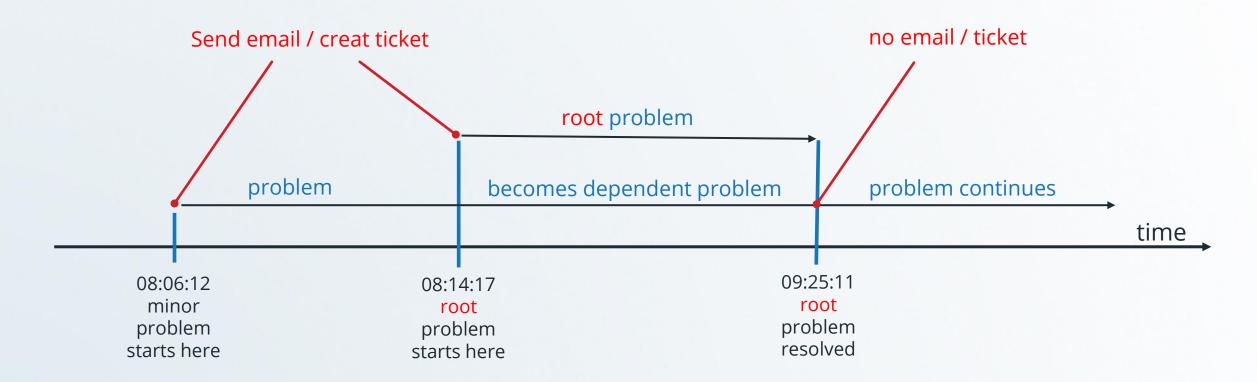
Severity	Name 🛦	Operational data	Expression
Average	SSH service is down Depends on: Ping and SSH: Unavailable by ICMP ping		max(/Ping and SSH/net.tcp.service[ssh],#3)=0
High	Unavailable by ICMP ping		max(/Ping and SSH/icmpping,#3)=0

Show	Recent problems Problems Hist	ory		Host inve						7	ABBIX
Host groups	type here to search		Select		Add					_	
Hosts	RHEL8 X		Select		Tags And/Or	Or					
	type here to search				tag						
Triggers	type here to search		Select								
Problem					Sho	w Recent problems	Problems Histo	bry		Host inventory	
Severity	Not classified Warning	High			Host group	type here to search			Select		Add
Gevenity	Information Average	Disaster			Hos	ts RHEL8 🗙			Select	Tags	And/Or Or
Age less then	14 days					type here to search					tag
Age less than	uays		Sho		Trigge	type here to search			Select		Add
					Proble	m				Show tags	None 1 2
					Severi	ty Not classified	Warning	High		Tag display priority	comma-separated
			Save			Information	Average	Disaster	Sho	w operational data	None Separa
			Save		Age less tha	an 🗌 14 day	/S		Show su	opressed problems	
Time v Severity Reco	overy time Status Info Host	Problem							0101/04		
12:07:29 High	RHEL8	1 Unavailable	e by ICMP ping 🔎							Compact view	
			×							Show details	
		Depende							Save as	Apply	Reset
0 selected Mass update		SSH ser	vice is down						Save as	Apply	teset
				Time 🔻 🗌	Severity Re	covery time Status	Info Host	Problem		Operational d	ata Duration
				12:07:29	High	12:08:13 RESOLVED	D RHEL8	1 Unavailat	ble by ICMP ping 🙎	Up (1)	44s
				12:07:09	Average	PROBLEM	RHEL8	SSH serv	vice 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?





Triggers do not overlap

Use case 1:

Different teams. Primary using emails/tickets to react Use case 2:

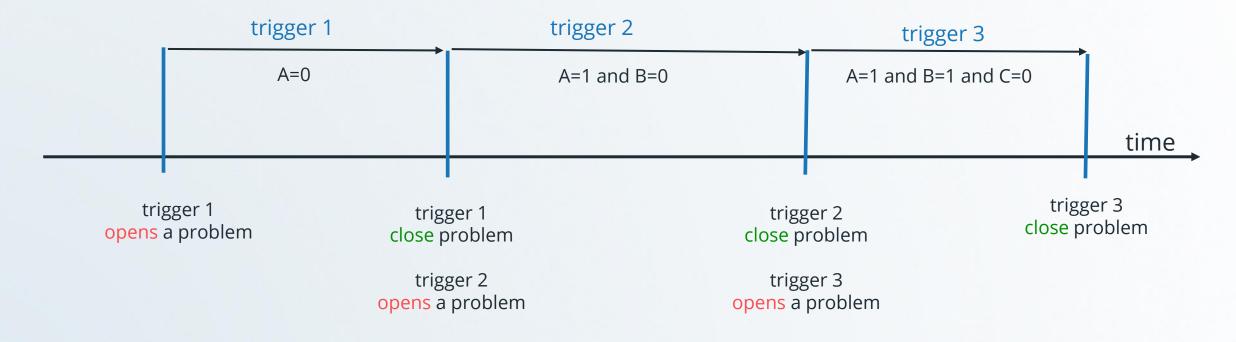
Doing a lot of agentless checks. Not using agents at all

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?

© 2023 by Zabbix. All rights reserved



Triggers do not overlap

Z	ABBIX « 🔊	Triggers		Create trigger
	Q	All templates / ICMP ping and SSH Items 2 Triggers 2 Graphs Dashboards Discovery rules Web scenarios		Filter T
0	Monitoring ~	Host groups type here to search Select Tags And/Or Or		
Ō	Services v	Templates ICMP ping and SSH × Select tag Contains value type here to search Add		Remove
≔	Inventory ~	type here to search Add Name Inherited all Yes No		
	Reports v	Severity Not classified Warning High With dependencies all Yes No		
4	Configuration ^	Information Average Disaster		
	Host groups	Status all Enabled Disabled		
	Templates	Apply Reset		
	Hosts			
	Maintenance	Severity Name Operational data Expression	Status	Tags
	Actions >	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
	Event correlation	High Unavailable by ICMP ping max(/ICMP ping and SSH/icmpping,#3)=0	Enabled	scope: availability
	Discovery			Displaying 2 of 2 found
•	Administration ~	0 selected Enable Disable Copy Mass update Delete		

Show	Recent problems Problems	listory		Host inventory	Туре				ZABBIX
Host groups	type here to search	S	Select		Add				
Hosts	RHEL8 X	S	Select	Tags	And/				
	type here to search				tag				
Triggers	type here to search	S	Select		Add				
Problem	1			Show tags	None				
Severity	Not classified Warning	High		Tag display priority	comm				
	Information Average	Disaster	S	how operational data	None				
Age less than	14 cays		Show s	5	Show	Recent problems	Problems History		Host inventory Type
					Host groups	type here to search		Select	Add
					Hosts			Select	Tags And
			Save as			type here to search			tag
					Triggers	type here to search		Select	Add
Time	Recovery time Status Info	Host Proble	lem		Problem				Show tags Non
13:00:20 Average	PROBLEM	RHEL8 SSH	service is down		Severity		Warning H	9	Tag display priority comn
						Information	Average D	isaster Sho	ow operational data Non
					Age less than	14 day	S	Show su	ippressed problems
									Compact view
									Show details
								Save as	Apply Reset
				Time 🔻 🗌	Severity Re	ecovery time Status	Info Host	Problem	Duration
				13:06:36 •	High	PROBLEI	M RHEL8	Unavailable by ICMP ping	1s
				13:00:20	Average	13:06:36 RESOLVE	ED RHEL8	SSH service is down	6m 16s

© 2023 by Zabbix. All rights reserved



Remove similar type of trigger

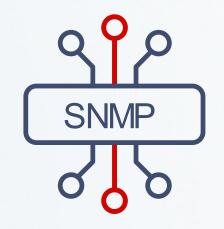
«SNMP availability» VS «ICMP ping»

- 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

Zł	ABBIX	≪ ₺	Triggers								?	Cre	ate trigger
		Q	All templates / Generic by	SNMP Items 12 Triggers 6	Graphs Dashboards	Discovery r	ules Web scenar	DS					Filter 🍸
⊞	Dashboard	s	Template gro	type here to search		Select		Tags And/Or Or					
0	Monitoring		Templa	tes Generic by SNMP × type here to search		Select		scope Add	Contains	 ✓ availability 	R	emove	
÷	Services		Na				Inh	erited all Yes No)				
≔	Inventory		Seve		Varning High		With depende	ncies all Yes No)				
J	Reports				Average Disa	aster							
Ŧ	Data collec	tion ^	Sta	tus all Enabled Disabl	ed								
	Template gro	oups					Apply	Reset					
	Host groups		Severity Name 🔺		Ope	erational data		Expression			Status	Tags	
	Templates			MP: No SNMP data collection	Cur	rent state: {ITE	M.LASTVALUE1}	max(/Generic by SNMP/	zabbix[host,snmp,available]],{\$SNMP.TIMEOUT}}=0	Enabled	scope: a	vailability
	Hosts Maintenance	;	Depends o Generic by	n: SNMP: Generic SNMP: Unavaila	ble by ICMP ping								
	Event correla		High Generic SN	MP: Unavailable by ICMP ping				max(/Generic by SNMP/i	cmpping,#3)=0		Enabled	scope: a	vailability
	Discovery										Dis	splaying 2	of 2 found
\bowtie	Alerts	~	0 selected Enable	Disable Copy Mass up	Delete								



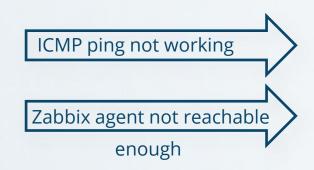
Remove similar type of triggers

«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	? Create item
All templates / Zabbix agent Items 4 Triggers 1 Graphs Dashboards 1 Discovery rules Web scenarios	Filter 🝸
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 <u>Triggers 1</u> zabbix[host,agent,available]	1m 7d 365d Zabbix internal Enabled component: system
Zabbix agent: Zabbix agent ping Severity Name	Expression Status
Average Zabbix agent: Zabbix agent	nt is not available max(/Zabbix agent/zabbix[host,agent,available],{\$AGENT.TIMEOUT})=0 Enabled
0 selected Enable Disable Copy Mass update Delete	
	All templates / Zabbix agent Items 4 Triggers 1 Graphs Dashboards 1 Discovery rules Web scenarios Name ▲ Triggers Key Sabbix agent: Host name of Zabbix agent running agent.hostname agent.version agent.version Zabbix agent: Zabbix agent availability Triggers 1 zabbix[host,agent,available] Zabbix agent: Zabbix agent ping Severity Name Average Zabbix agent: Zabbix agent: Zabbix agent ping Severity Name

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

© 2023 by Zabbix. All rights reserved



Global correlation

Use case:

✤ Device hierarchy. ISP situation

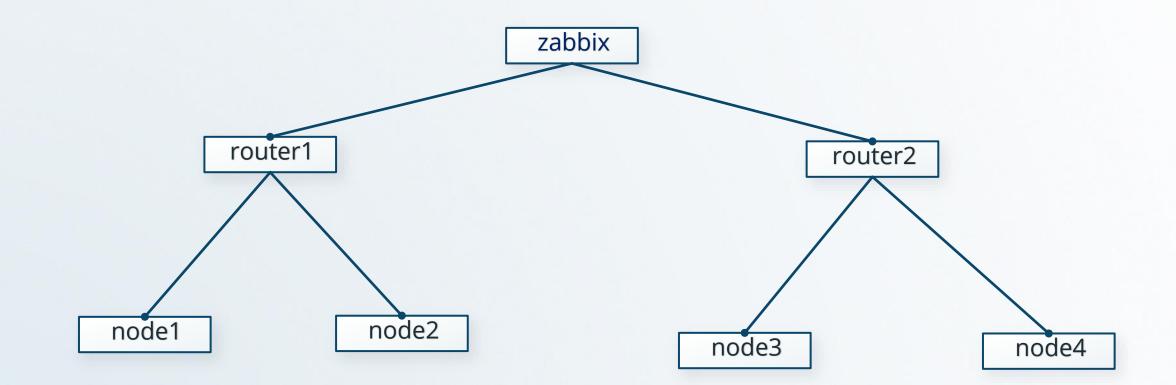
Availability trigger is critical

Cons

Will pile up database very fast - slow down GUI experience

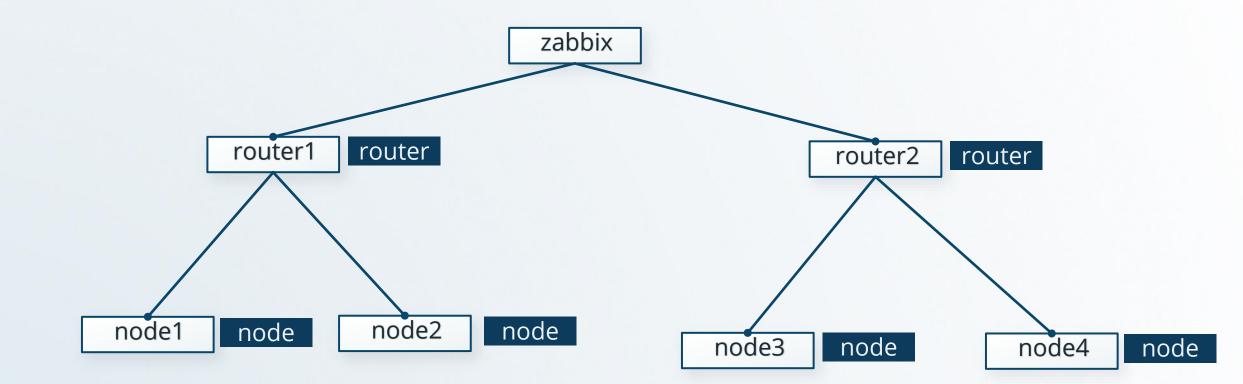
- ✤Will generate an unexpected CPU load
- **~** Safer to use with a new deployment





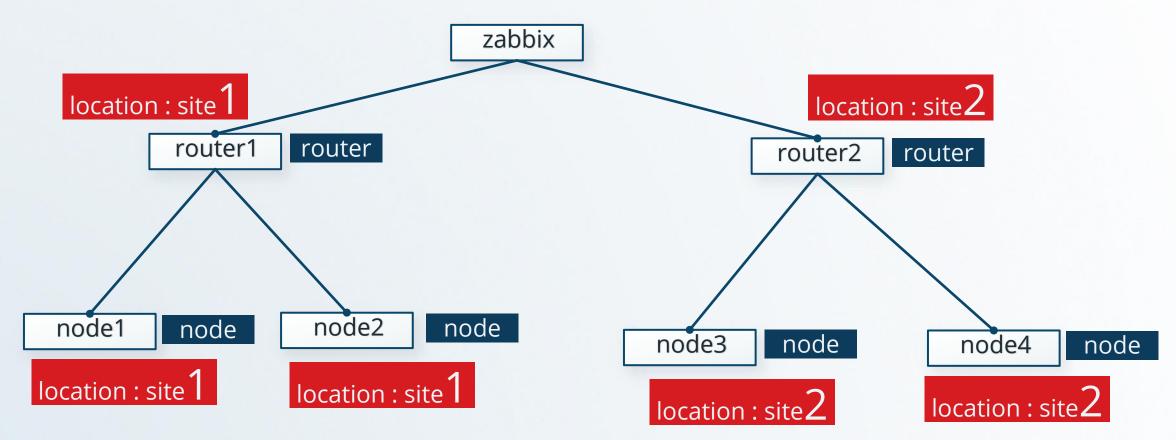
Availability check





Create a tag without a value





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



Z	ABBIX « 🔊	Event correlation		?	Create correlation
	Q				Filter 🍸
⊞	Dashboards		Name Status Any Enabled Disabled		
$^{\odot}$	Monitoring		Apply Reset		
品	Services				
		Name ▲	Conditions	Operations	Status
≣	Inventory	root cause after symptoms	Value of old event tag location equals value of new event tag location	Close old events	Enabled
J	Reports		New event tag name equals <i>router</i> Old event tag name equals <i>node</i>		
ځ	Data collection	symptoms after root cause	Value of old event tag <i>location</i> equals value of new event tag <i>location</i> New event tag name equals <i>node</i>	Close new event	Enabled
	Template groups		Old event tag name equals router		
	Host groups				Displaying 2 of 2 found
	Templates	0 selected Enable Disable Delete			
	Hosts				
	Maintenance				
	Event correlation				
	Discovery				

We do not need to hardcode the location value



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)

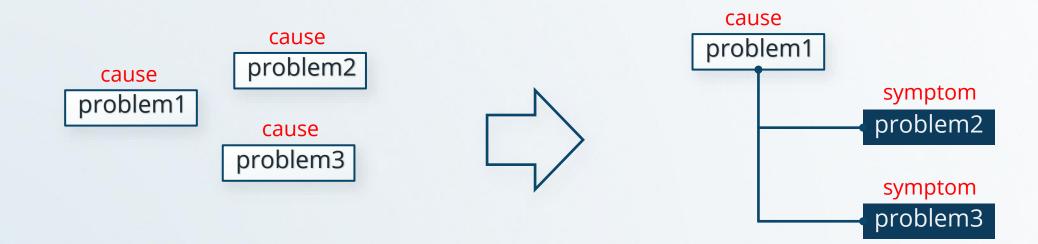
Cons

- 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»

Droblomo

=	Probl	ems									
<	7										
		Time 🔻	Severity	Recovery time	Status	Info	Host	Problem		Du	iration
•		18:15:01	Not classified				Zabbix server	Application una	vailable on (23)	1m	14s
✓		18:15:01	Not classified				Zabbix server	Host (23) unava	ailable	1m	n 4s
		18:15:01	Not classified				Zabbix server	Power outage		1m	4s
		Today ㅇ							VIEW		
	2022-10-	17 10:38:52	Average		PROBLEM		Zabbix server	1 Interface e	History	►	13d 8h
		October •							CONFIGURATION		
	2022-09-	16 12:38:25	Not classified		PROBLEM		Zabbix server	A class: trigge	Trigger		14d 6h
	2022-09-	16 12:12:47	Not classified		PROBLEM		Zabbix server	A class: trigge	Items	•	14d 7h
	2022-09-	16 12:09:28	Not classified		PROBLEM		Zabbix server	A class: trigge	PROBLEM		14d 7h
	2022-09-	16 12:04:06	Not classified		PROBLEM		Zabbix server	A class: trigge	Mark as cause Mark selected as symptoms		14d 7h
	2022-09-	16 11:59:30	Not classified	S ZUZO L	PROBI FM		Zabbix server	A class: trigge	In annuel anne va	- 314	14d 7h



Thank you!

Aigars Kadikis

Technical Support Engineer & Zabbix Trainer