1. Create item and develop custom trigger for log monitoring (you can use httpd or tomcat logs)

[root@pdv-zabclnt lib]# chmod +rx /var/log/tomcat/

2. Create a trigger for errors in log file monitored by that item

pdv-zabclnt: Log tomcat access

View as Values

Zoom out Last 15 minutes

From now-15m
To now

Apply

Last 2 days Yesterday Today
Last 7 days Day before yesterday Today so far
Last 30 days This day last week This week
Last 3 months Previous week This week so far
Last 6 months Previous month This month
Last 1 year Previous year This month so far
Last 2 years This year
This year so far

```
192.168.56.201 - - [21/Oct/2019:10:09:01 +0000] "GET / HTTP/1.1" 200 11217
192.168.56.201 - - [21/Oct/2019:10:09:01 +0000] "GET /TestApp/ HTTP/1.1" 200 813
192.168.56.1 - - [21/Oct/2019:13:52:16 +0000] "GET / HTTP/1.1" 200 11217
192.168.56.1 - - [21/Oct/2019:13:52:16 +0000] "GET /asf-logo-wide.svg HTTP/1.1" 200 26447
192.168.56.1 - - [21/Oct/2019:13:52:25 +0000] "GET /TestApp HTTP/1.1" 302 -
192.168.56.1 - - [21/Oct/2019:13:52:25 +0000] "GET /TestApp/ HTTP/1.1" 200 813
192.168.56.1 - - [21/Oct/2019:13:52:25 +0000] "GET /TestApp/css/bootstrap.min.cs s HTTP/1.1" 200 121200
192.168.56.1 - - [21/Oct/2019:13:52:25 +0000] "GET /TestApp/js/bootstrap.min.js HTTP/1.1" 200 37045
192.168.56.1 - - [21/Oct/2019:13:52:25 +0000] "GET /TestApp/css/bootstrap-theme. min.css HTTP/1.1" 200 23409
192.168.56.1 - - [21/Oct/2019:13:52:25 +0000] "GET /TestApp/js/jquery-3.2.1.js H TTP/1.1" 200 268039
192.168.56.1 - - [21/Oct/2019:13:52:27 +0000] "GET /TestApp/generic.jsp HTTP/1.1 " 200 1134
192.168.56.1 - - [21/Oct/2019:15:24:48 +0000] "GET /TestApp HTTP/1.1" 302 -
192.168.56.1 - - [21/Oct/2019:15:24:48 +0000] "GET /TestApp/ HTTP/1.1" 200 813
192.168.56.1 - - [21/Oct/2019:15:24:51 +0000] "GET /TestApp1 HTTP/1.1" 404 967
192.168.56.1 - - [21/Oct/2019:15:31:13 +0000] "GET /TestApp1 HTTP/1.1" 404 967
192.168.56.1 - - [21/Oct/2019:15:31:14 +0000] "GET /TestApp1 HTTP/1.1" 404 967
<log/tomcat/localhost_access_log.2019-10-21.txt" 955L, 75365C 955,1        Bot
```

Timestamp	Local time	Value
2019-10-21 18:31:44		192.168.56.1 - - [21/Oct/2019:15:31:14 +0000] "GET /TestApp1 HTTP/1.1" 404 967
2019-10-21 18:31:44		192.168.56.1 - - [21/Oct/2019:15:31:13 +0000] "GET /TestApp1 HTTP/1.1" 404 967
2019-10-21 18:25:14		192.168.56.1 - - [21/Oct/2019:15:24:48 +0000] "GET /TestApp/ HTTP/1.1" 200 813

Z Zabbix Server: Configuratio × +

← → C ⟳ ① Not secure | 192.168.56.201/triggers.php?groupid=0&hostid=10263

☐	Information	OK	Template App Zabbix Agent: Host name of zabbix_agent was changed on {HOST.NAME}	{pdv-zabclnt:agent.hostname.**diff**(0)}>0	Enabled
☐	Information	OK	Template OS Linux: Hostname was changed on {HOST.NAME}	{pdv-zabclnt:system.hostname.**diff**(0)}>0	Enabled
☐	Average	OK	Template OS Linux: Lack of available memory on server {HOST.NAME}	{pdv-zabclnt:vm.memory.size[available].**last**(0)}<20M	Enabled
☐	Warning	OK	Template OS Linux: Lack of free swap space on {HOST.NAME}	{pdv-zabclnt:system.swap.size[,pfree].**last**(0)}<50	Enabled
☐	Warning	OK	Template OS Linux: Processor load is too high on {HOST.NAME}	{pdv-zabclnt:system.cpu.load[percpu,avg1].**avg**(5m)}>5	Enabled
☐	Not classified	OK	Someone want to view our app	Problem: {pdv-zabclnt:log[/var/log/tomcat/localhost_access_log.2019-10-21.txt,"HTTP",,,,].**regexp**(200,30)}=1 Recovery: {pdv-zabclnt:log[/var/log/tomcat/localhost_access_log.2019-10-21.txt,"HTTP",,,,].**regexp**(200,30)}=0	Enabled

Please configure:
1. Simple checks: Zabbix DB is available (3306)

All hosts / Zabbix server Enabled ZBX SNMP JMX IPMI Applications 12 Items 89 Triggers 51 Graphs 15 Discovery rules 2 Web scenarios

Item Preprocessing

* Name Check mysql
Type Simple check ▼
* Key net.tcp.service[tcp,127.0.0.1,3306] Select
* Host interface 127.0.0.1 : 10050 ▼

Zabbix server: Check mysql

	last	min	avg	max
☐ Check mysql [all]	1	1	1	1
◉ Trigger: DB is unavailable [= 0]				

	Severity	Value	Name ▲	Expression	Status	
☐	Warning	OK	Template OS Linux: /etc/passwd has been changed on {HOST.NAME}	{Zabbix server:vfs.file.cksum[/etc/passwd].**diff**(0)}>0	Enabled	
☐	Information	OK	Template OS Linux: Configured max number of opened files is too low on {HOST.NAME}	{Zabbix server:kernel.maxfiles.**last**(0)}<1024	Enabled	
☐	Information	OK	Template OS Linux: Configured max number of processes is too low on {HOST.NAME}	{Zabbix server:kernel.maxproc.**last**(0)}<256	Enabled	
☐	High	OK	DB is unavailable	Problem: {Zabbix server:net.tcp.service[tcp,127.0.0.1,3306].**last**(,30)}=0 Recovery: {Zabbix server:net.tcp.service[tcp,127.0.0.1,3306].**last**(,30)}=1	Enabled	

	High	PROBLEM	DB is unavailable	Problem: {Zabbix server:net.tcp.service[tcp,127.0.0.1,3306].**last**(,30)}=0 Recovery: {Zabbix server:net.tcp.service[tcp,127.0.0.1,3306].**last**(,30)}=1	Enabled

Zabbix server: Check mysql

	last	min	avg	max
■ Check mysql [all]	1	0	0.3333	1
○ Trigger: DB is unavailable [= 0]				
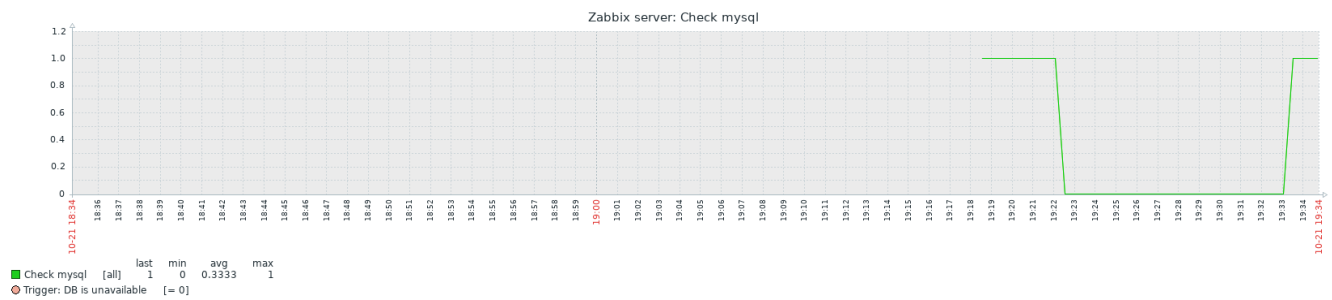
2. Calculated Checks: CPU Load per Core (1, 5, 15min)

Items

All hosts / pdv-zabclnt   Enabled   ZBX SNMP JMX IPMI   Applications 11   Items 54   Triggers 20   Graphs 9   Discovery rules 2   Web scenarios

Item   Preprocessing

Parent items	Template OS Linux
* Name	cpu load 1 min
Type	Zabbix agent
* Key	system.cpu.load[,avg1]
* Host interface	192.168.56.203 : 10050
* Type of information	Numeric (float)

ZABBIX   Monitoring   Inventory   Reports   Configuration   Administration   🔍 🎧 Support

Host groups   Templates   Hosts   Maintenance   Actions   Event correlation   Discovery   Services

Items

All hosts / pdv-zabclnt   Enabled   ZBX SNMP JMX IPMI   Applications 11   Items 54   Triggers 20   Graphs 9   Discovery rules 2   Web scenarios

Item   Preprocessing

* Name	CPU Load per Core (1 min)
Type	Calculated
* Key	system.load.core[1min]
* Formula	last("system.cpu.load[,avg1]")/last("system.cpu.num[]")

Host	Name ▲	Last check	Last value	Change	
▼ ☐					
▼ pdv-zabclnt	**cpu_load** (7 Items)				
☐	cpu load 1 min	2019-10-21 20:27:12	0		Graph
☐	cpu load 5 min	2019-10-21 20:26:45	0.01		Graph
☐	cpu load 15 min	2019-10-21 20:26:48	0.05		Graph
☐	CPU Load per Core (1 min)	2019-10-21 20:26:49	0		Graph
☐	CPU Load per Core (5 min)	2019-10-21 20:26:50	0.005		Graph
☐	CPU Load per Core (15 min)	2019-10-21 20:26:51	0.03		Graph
☐	number of cpus	2019-10-21 20:27:09	2		Graph

pdv-zabclnt: CPU Load per Core (1 min)

	last	min	avg	max
■ CPU Load per Core (1 min) [all]	0	0	0.0156	0.04

Items

All hosts / pdv-zabclnt   Enabled   ZBX SNMP JMX IPMI   Applications 11   Items 54   Triggers 20   Graphs 9   Discovery rules 2   Web scenarios

Item   Preprocessing

* Name: CPU Load per Core (15 min)

Type: Calculated ▼

* Key: system.load.core[15min]   [Select]
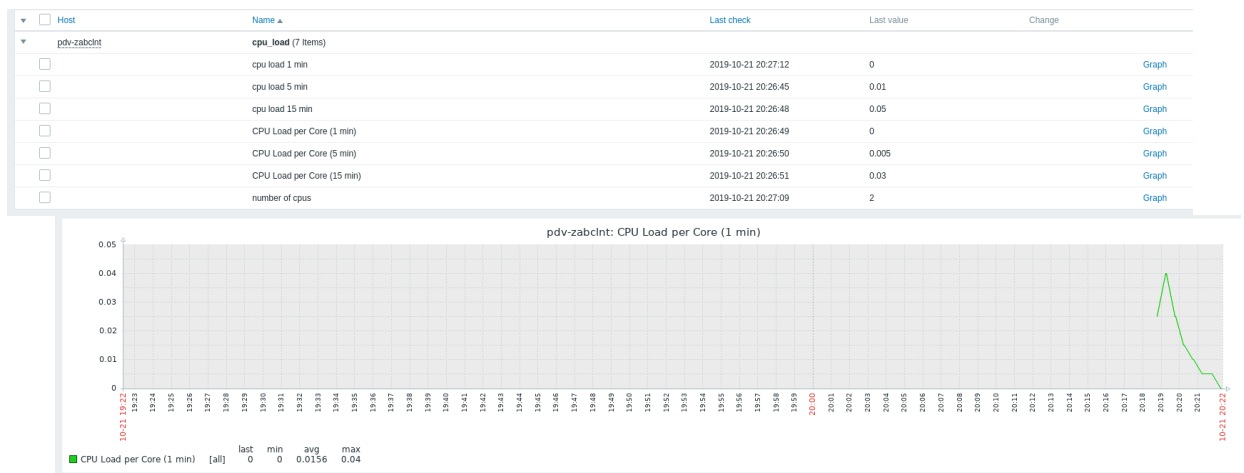
* Formula: last("system.cpu.load[,avg15]")/last("system.cpu.num[]")

Type of information: Numeric (float) ▼

Units:

* Update interval: 30s

Host groups   Templates   **Hosts**   Maintenance   Actions   Event correlation   Discovery   Services

Items

All hosts / pdv-zabclnt   Enabled   ZBX SNMP JMX IPMI   Applications 11   Items 54   Triggers 20   Graphs 9   Discovery rules 2   Web scenarios

Item   Preprocessing

* Name   CPU Load per Core (5 min)

Type   Calculated ▼

* Key   system.load.core[5min]   Select

* Formula   last("system.cpu.load[,avg5]")/last("system.cpu.num[]")

Trigger:

Host groups   Templates   **Hosts**   Maintenance   Actions   Event correlation   Discovery   Services

Triggers

All hosts / pdv-zabclnt   Enabled   ZBX SNMP JMX IPMI   Applications 11   Items 54   Triggers 20   Graphs 9   Discovery rules 2   Web scenarios

Trigger   Dependencies

* Name   CPU load is high

Severity   Not classified   Information   Warning   Average   **High**   Disaster

* Problem expression   {pdv-zabclnt:system.load.core[1min].last(,30)}>0.1   Add

Expression constructor

OK event generation   Expression   Recovery expression   None

* Recovery expression   {pdv-zabclnt:system.load.core[1min].last(,30)}<0.1   Add

Expression constructor

PROBLEM event generation mode   Single   Multiple

OK event closes   All problems   All problems if tag values match

Tags   tag   value   Remove

Add

High	OK	CPU load is high	Problem: {pdv-zabclnt:system.load.core[1min].last(,30)}>0.1	Enabled
			Recovery: {pdv-zabclnt:system.load.core[1min].last(,30)}<0.1	

pdv-zabclnt: cpu load 1 min

| cpu load 1 min [all] | last 0.42 | min 0 | avg 0.0195 | max 0.42 |

| | High | PROBLEM | CPU load is high | Problem: {pdv-zabclnt:system.load.core[1min].last(,30)}>0.1 | Enabled |
| | | | | Recovery: {pdv-zabclnt:system.load.core[1min].last(,30)}<0.1 | |

Global view

All dashboards / Global view

System information

Parameter	Value	Details
Zabbix server is running	Yes	pdv-zabserv:10051
Number of hosts (enabled/disabled/templates)	83	2 / 0 / 81
Number of items (enabled/disabled/not supported)	147	142 / 0 / 5
Number of triggers (enabled/disabled [problem/ok])	72	72 / 0 [2 / 70]
Number of users (online)	2	1
Required server performance, new values per second	2.22	

Problems by severity

Host group ▲	Disaster	High	Average	Warning	Information	Not classified
CloudHosts		1				1

Loc

Problems

Time ▼	Info	Host	Problem • Severity	Duration	Ack	Actions	Tags
20:44:19		pdv-zabclnt	CPU load is high	30s	No		
20:43:15		pdv-zabclnt	Someone want to view our app	1m 34s	No		

Fav

| | High | OK | CPU load is high | Problem: {pdv-zabclnt:system.load.core[1min].last(,30)}>0.1 | Enabled |
| | | | | Recovery: {pdv-zabclnt:system.load.core[1min].last(,30)}<0.1 | |

	cpu load 1 min	2019-10-21 20:52:12	0	-0.01	Graph
	cpu load 5 min	2019-10-21 20:51:45	0.18	-0.02	Graph
	cpu load 15 min	2019-10-21 20:51:48	0.17	-0.01	Graph
	CPU Load per Core (1 min)	2019-10-21 20:51:49	0.005		Graph
	CPU Load per Core (5 min)	2019-10-21 20:51:50	0.09	-0.01	Graph
	CPU Load per Core (15 min)	2019-10-21 20:51:51	0.09		Graph
	number of cpus	2019-10-21 20:52:09	2		Graph

0 selected   Display stacked graph   Display graph

Triggers

All hosts / pdv-zabclnt   Enabled   ZBX SNMP JMX IPMI   Applications 11   Items 54   Triggers 23   Graphs 9   Discovery rules 2   Web scenarios

Trigger   Dependencies

* Name	CPU load is high 5 min

Severity   [Not classified] [Information] [Warning] [Average] [High] [Disaster]

* Problem expression

{pdv-zabclnt:system.load.core[5min].last(,30)}>0.3

Add

Expression constructor

OK event generation   [Expression] [Recovery expression] [None]

* Recovery expression

{pdv-zabclnt:system.load.core[5min].last(,30)}<0.3

Add

Expression constructor

Triggers

All hosts / pdv-zabclnt   Enabled   **ZBX** SNMP JMX IPMI   Applications 11   Items 54   Triggers 23   Graphs 9   Discovery rules 2   Web scenarios

Trigger   Dependencies

* Name	CPU load is high 15 min
Severity	Not classified | Information | Warning | Average | High | Disaster
* Problem expression	{pdv-zabclnt:system.load.core[15min].last(,30)}>0.3 [Add]

Expression constructor

OK event generation	Expression | Recovery expression | None
* Recovery expression	{pdv-zabclnt:system.load.core[15min].last(,30)}<0.3 [Add]

Expression constructor

PROBLEM event generation mode	Single | Multiple
OK event closes	All problems | All problems if tag values match
Tags	tag value Remove

Add

3. Internal Checks: How many items are enabled

All hosts / pdv-zabclnt   Enabled   **ZBX** SNMP JMX IPMI   Applications 12   Items 55   Triggers 23   Graphs 9   Discovery rules 2   Web scenarios
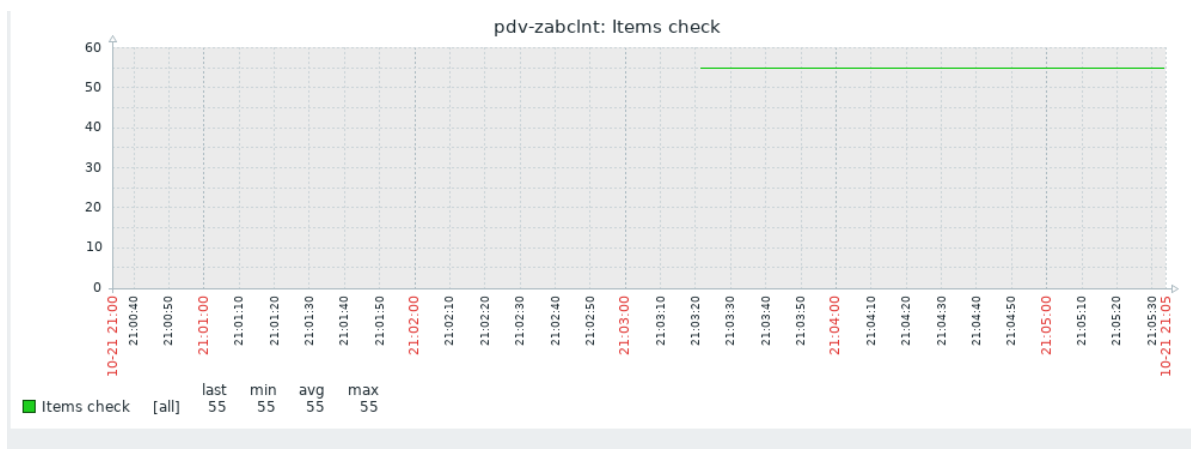
Item   Preprocessing

* Name	Items check
Type	Zabbix internal ▼
* Key	zabbix[host,,items] [Select]
Type of information	Numeric (unsigned) ▼
Units	
* Update interval	30s

pdv-zabclnt: Items check

	last	min	avg	max
Items check [all]	55	55	55	55

Host groups   Templates   **Hosts**   Maintenance   Actions   Event correlation   Discovery   Services

Triggers

All hosts / pdv-zabclnt   Enabled   **ZBX** SNMP JMX IPMI   Applications 12   Items 55   **Triggers** 23   Graphs 9   Discovery rules 2   Web scenarios

Trigger   Dependencies

* Name	Check of number items on host

Severity   [Not classified] [Information] [Warning] [Average] [High] [Disaster]

* Problem expression

```
{pdv-zabclnt:zabbix[host,,items].last(,30)}<55
```
[Add]

Expression constructor

OK event generation   [Expression] [Recovery expression] [None]

* Recovery expression

```
{pdv-zabclnt:zabbix[host,,items].last(,30)}>=55
```
[Add]

Expression constructor

PROBLEM event generation mode   [Single] [Multiple]

OK event closes   [All problems] [All problems if tag values match]

Tags   [tag]   [value]   Remove

	Wizard	Name ▲	Triggers	Key	Interval	History	Trends	Type	Applications	Status	Info
☐	•••	Template App Zabbix Agent: Agent ping	Triggers 1	agent.ping	1m	1w	365d	Zabbix agent	Zabbix agent	Disabled	
☐	•••	Template OS Linux: Available memory	Triggers 1	vm.memory.size[available]	1m	1w	365d	Zabbix agent	Memory	Enabled	
☐	•••	Template OS Linux: Checksum of /etc/passwd	Triggers 1	vfs.file.cksum[/etc/passwd]	1h	1w	365d	Zabbix agent	Security	Enabled	
☐	•••	Template OS Linux: Context switches per second		system.cpu.switches	1m	1w	365d	Zabbix agent	CPU, Performance	Enabled	

☐	Not classified	PROBLEM	Check of number items on host	Problem: {pdv-zabclnt:zabbix[host,,items].last(,30)}<55	Enabled
				Recovery: {pdv-zabclnt:zabbix[host,,items].last(,30)}>=55	

System information   ...

Parameter	Value	Details
Zabbix server is running	Yes	pdv-zabserv:10051
Number of hosts (enabled/disabled/templates)	83	2 / 0 / 81
Number of items (enabled/disabled/not supported)	148	142 / 1 / 5
Number of triggers (enabled/disabled [problem/ok])	75	74 / 1 [1 / 73]
Number of users (online)	2	1
Required server performance, new values per second	2.23	

Problems by severity   ...

Host group ▲	Disaster	High	Average	Warning	Information	Not classified
CloudHosts						1

Problems   ...

	Time ▼	Info	Host	Problem • Severity	Duration	Ack	Actions	Tags
	21:10:52		pdv-zabclnt	Check of number items on host	4m 12s	No		

Internal Checks: How many Servers are being monitored

Host groups   Templates   **Hosts**   Maintenance   Actions   Event correlation   Discovery   Services

Items

All hosts / Zabbix server   Enabled   **ZBX** SNMP JMX IPMI   Applications 13   Items 93   Triggers 51   Graphs 15   Discovery rules 2   Web scenarios

Item   Preprocessing

* Name	Number of monitored hosts
Type	Zabbix internal ▼
* Key	zabbix[hosts] Select
Type of information	Numeric (unsigned) ▼
Units	
* Update interval	30s

Custom intervals

Type	Interval	Period	Action
Flexible Scheduling	50s	1-7,00:00-24:00	Remove

Add

* History storage period	90d
* Trend storage period	365d
Show value	As is ▼ show value mappings
New application	Internal check
Applications	-None- CPU

Triggers

All hosts / Zabbix server   Enabled   ZBX SNMP JMX IPMI   Applications 14   Items 94   Triggers 51   Graphs 15   Discovery rules 2   Web scenarios

Trigger   Dependencies

* Name	Not all servers are monitored
Severity	Not classified Information Warning Average High Disaster
* Problem expression	{Zabbix server:zabbix[hosts].last(,30)}<2 Add

Expression constructor

OK event generation	Expression Recovery expression None
* Recovery expression	{Zabbix server:zabbix[hosts].last(,30)}=2 Add

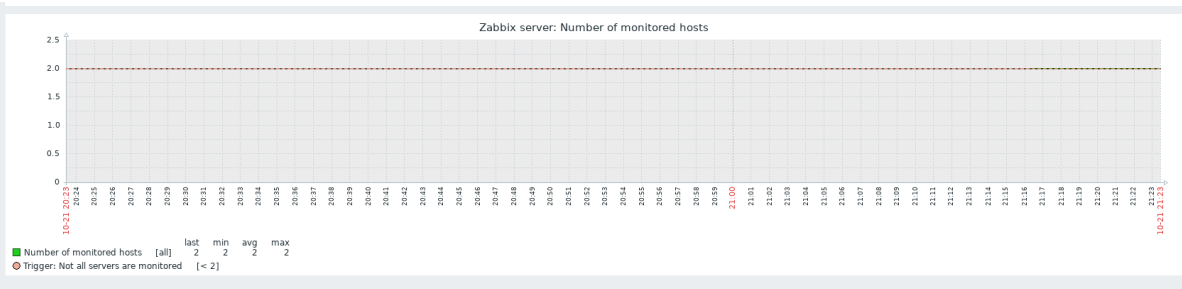Expression constructor

PROBLEM event generation mode   Single   Multiple

Zabbix server: Number of monitored hosts

2.5
2.0
1.5
1.0
0.5
0

10-21 20:23 20:24 20:25 20:27 20:29 20:30 20:31 20:32 20:33 20:34 20:35 20:36 20:37 20:38 20:39 20:40 20:41 20:42 20:43 20:44 20:45 20:46 20:47 20:48 20:49 20:50 20:51 20:52 20:53 20:54 20:55 20:56 20:57 20:58 20:59 21:00 21:01 21:02 21:03 21:04 21:05 21:06 21:07 21:08 21:09 21:10 21:11 21:12 21:13 21:14 21:15 21:16 21:17 21:18 21:19 21:20 21:21 21:22 21:23 10-21 21:23

	last	min	avg	max
■ Number of monitored hosts [all]	2	2	2	2
● Trigger: Not all servers are monitored [< 2]				

Hosts

Group all ▼   Create host   Import

Filter ▼

Name		DNS	
Monitored by	Any Server Proxy	IP	
		Port	

Apply   Reset

	Name ▲	Applications	Items	Triggers	Graphs	Discovery	Web	Interface	Templates	Status	Availability	Agent encryption	Info
☐	pdv-zabclnt	Applications 12	Items 55	Triggers 24	Graphs 9	Discovery 2	Web	192.168.56.203: 10050	Template OS Linux (Template App Zabbix Agent)	Disabled	ZBX SNMP JMX IPMI	NONE	

☐	High	PROBLEM	Not all servers are monitored		Problem: {Zabbix server:zabbix[hosts].last(,30)}<2 Recovery: {Zabbix server:zabbix[hosts].last(,30)}=2	Enabled

---

Problems

	Time ▼	Info	Host	Problem • Severity	Duration	Ack	Actions	Tags
	21:31:23		Zabbix server	Not all servers are monitored	37s	No		

	Name ▲	Applications	Items	Triggers	Graphs	Discovery	Web	Interface	Templates	Status	Availability	Agent encryption	Info
☐	pdv-zabclnt	Applications 12	Items 55	Triggers 24	Graphs 9	Discovery 2	Web	192.168.56.203: 10050	Template OS Linux (Template App Zabbix Agent)	Enabled	ZBX SNMP JMX IPMI	NONE	

Zabbix server: Number of monitored hosts

		last	min	avg	max
■ Number of monitored hosts	[all]	2	1	1.73	2
⊙ Trigger: Not all servers are monitored	[< 2]				

☐	High	OK	Not all servers are monitored	Problem: {Zabbix server:zabbix[hosts].**last**(,30)}<2	Enabled
				Recovery: {Zabbix server:zabbix[hosts].**last**(,30)}=2	