

## Opensource ICT Solutions

# ZABBIX Meet up

# How to get most out of Zabbix problems

- Microphones are muted
- Ask your questions in Q&A, not in the chat





# Laura Schilder

Zabbix Consultant



## OpenSource ICT Solutions

Your Zabbix partner in:

- The Netherlands
- United Kingdom
- United States



Windows by Zabbix agent: System time is out of sync

```
fuzzytime(/Windows client/system.localtime,{SYSTEM.FUZZYTIME.MAX})=0
```

## • What is an trigger?

Parent triggers [Windows by Zabbix agent](#)

\* Name

Event name

Operational data

Severity

\* Expression

[Expression constructor](#)



# A problem arises, now what?

- Identify the problem
- What is the problem about?
- Do you know what to do now?



# What are problems?

- Trigger > problem state
- Indicating something(bad) that might need our attention
- Can be informational

Time	Severity	Recovery time	Status	Info	Host	Problem	Duration	Ack	Actions	Tags
14:13:00	Average		PROBLEM		Windows client	<a href="#">\\192.168.1.74\public\test1356.txt: Is older than 15 minutes</a>	1h 20m 50s	No		class: service component: storage scope: notice ...
14:00										
11:45:00	Average		PROBLEM		Windows client	<a href="#">\\192.168.1.74\public\test: Is older than 15 minutes</a>	3h 48m 50s	No		class: service component: storage scope: notice ...
Today										
2022-11-14 12:55:29	Average		PROBLEM		Windows client	<a href="#">This file has been around for more then 15 minutes</a>	8d 2h 38m	No		class: service component: storage scope: notice ...
2022-11-14 12:55:29	Average		PROBLEM		Windows client	<a href="#">This file has been around for more then 15 minutes</a>	8d 2h 38m	No		class: service component: storage scope: notice ...
2022-11-14 12:55:29	Average		PROBLEM		Windows client	<a href="#">This file has been around for more then 15 minutes</a>	8d 2h 38m	No		class: service component: storage scope: notice ...
2022-11-14 12:55:29	Average		PROBLEM		Windows client	<a href="#">This file has been around for more then 15 minutes</a>	8d 2h 38m	No		class: service component: storage scope: notice ...
2022-11-14 12:55:00	Average		PROBLEM		Windows client	<a href="#">\\192.168.1.74\public\file1158: Is older than 15 minutes</a>	8d 2h 38m	No		class: service component: storage scope: notice ...



# How to alert about them?

- What are the options?
- Global notifications
- Send messages
- Create tickets
- Execute remote commands



# Global notifications

- What are they?
- Can be displayed everywhere in Zabbix
- Move
- Mute
- Snooze

User profile: Zabbix Administrator ▾

User Media Messaging ●

Frontend messaging

Message timeout

Play sound

Trigger severity

<input type="checkbox"/> Recovery	<input type="text" value="alarm_ok"/>	<input type="button" value="Play"/>	<input type="button" value="Stop"/>
<input type="checkbox"/> Not classified	<input type="text" value="no_sound"/>	<input type="button" value="Play"/>	<input type="button" value="Stop"/>
<input type="checkbox"/> Information	<input type="text" value="alarm_information"/>	<input type="button" value="Play"/>	<input type="button" value="Stop"/>
<input checked="" type="checkbox"/> Warning	<input type="text" value="no_sound"/>	<input type="button" value="Play"/>	<input type="button" value="Stop"/>
<input checked="" type="checkbox"/> Average	<input type="text" value="no_sound"/>	<input type="button" value="Play"/>	<input type="button" value="Stop"/>
<input type="checkbox"/> High	<input type="text" value="alarm_high"/>	<input type="button" value="Play"/>	<input type="button" value="Stop"/>
<input type="checkbox"/> Disaster	<input type="text" value="alarm_disaster"/>	<input type="button" value="Play"/>	<input type="button" value="Stop"/>

Show suppressed problems

Problem on Windows client  
C:\share\temp\_stuff\o.bmp: Is older than 15 minutes  
2022-11-14 11:03:29

Problem on Windows client  
C:\share\temp\_stuff\b.rtf: Is older than 15 minutes  
2022-11-14 11:03:29

Problem on Windows client  
C:\share\temp\_stuff\a.txt: Is older than 15 minutes  
2022-11-14 11:03:29

Problem on Windows client  
C:\share\temp\_stuff\a.png: Is older than 15 minutes  
2022-11-14 11:03:29

Problem on Windows client  
\\192.168.1.74\public\test1356.txt: Is older than 15 minutes  
2022-11-14 11:03:00

Problem on Windows client  
\\192.168.1.74\public\test: Is older than 15 minutes  
2022-11-14 11:03:00

Problem on Windows client  
\\192.168.1.74\public\file1158: Is older than 15 minutes  
2022-11-14 11:03:00

# Media types/ Send messages

- Administration -> Media types
- Email
- Sms
- Webhook
- Script

Media types

Name  Status Any Enabled Disabled

<input type="checkbox"/> Name ▲	Type	Status	Used in actions	Details
<input type="checkbox"/> Brevis.one	Webhook	<a href="#">Enabled</a>		
<input type="checkbox"/> Discord	Webhook	<a href="#">Enabled</a>		
<input type="checkbox"/> Email	Email	<a href="#">Enabled</a>		SMTP server: "mail.example.com", SMTP helo: "example.com", SMTP email: "zabbix@example.com"
<input type="checkbox"/> Email (HTML)	Email	<a href="#">Enabled</a>		SMTP server: "mail.example.com", SMTP helo: "example.com", SMTP email: "zabbix@example.com"
<input type="checkbox"/> Express.ms	Webhook	<a href="#">Enabled</a>		
<input type="checkbox"/> Github	Webhook	<a href="#">Enabled</a>		
<input type="checkbox"/> GLPI	Webhook	<a href="#">Enabled</a>		
<input type="checkbox"/> ILert	Webhook	<a href="#">Enabled</a>		
<input type="checkbox"/> ITop	Webhook	<a href="#">Enabled</a>		
<input type="checkbox"/> Jira	Webhook	<a href="#">Enabled</a>		
<input type="checkbox"/> Jira ServiceDesk	Webhook	<a href="#">Enabled</a>		



- How?
- Via what?
- Wich day/time do you prefer?

### Media

Type

\* Send to  [Remove](#)

[Add](#)

\* When active

Use if severity  Not classified  
 Information  
 Warning  
 Average  
 High  
 Disaster

Enabled

- Why get an message if you can get a ticket?
- What?
- Choose which ticketing software you like
- Escalation



# Presenting problems

- What is this problem?
- Naming
- Tagging
- Dashboard/widgets
- Frontend filters



# Naming

- Keep it simple and understandable
- Don't make them too long
- Macro's

Average	PROBLEM	Discover time: C:\share\temp_stufflo.bmp: Is older than 15 minutes	fuzzytime(/Windows client/time.access["C:\share\temp_stufflo.bmp"],15m)=0	Enabled	scope: notice
Average	PROBLEM	Discover time network: \\192.168.1.74\publicfile1158: Is older than 15 minutes	fuzzytime(/Windows client/time.access["\\192.168.1.74\publicfile1158"],15m)=0	Enabled	scope: notice



PROBLEM Windows client This file has been around for more then 15 minutes

<input type="checkbox"/>	Severity	Name ▲
<input type="checkbox"/>	Average	{#TEMPFILENAME}: Is older than 15 minutes



Discover time: C:\share\temp\_stufflo.bmp: Is older than 15 minutes



- Use scope

- Need more information?

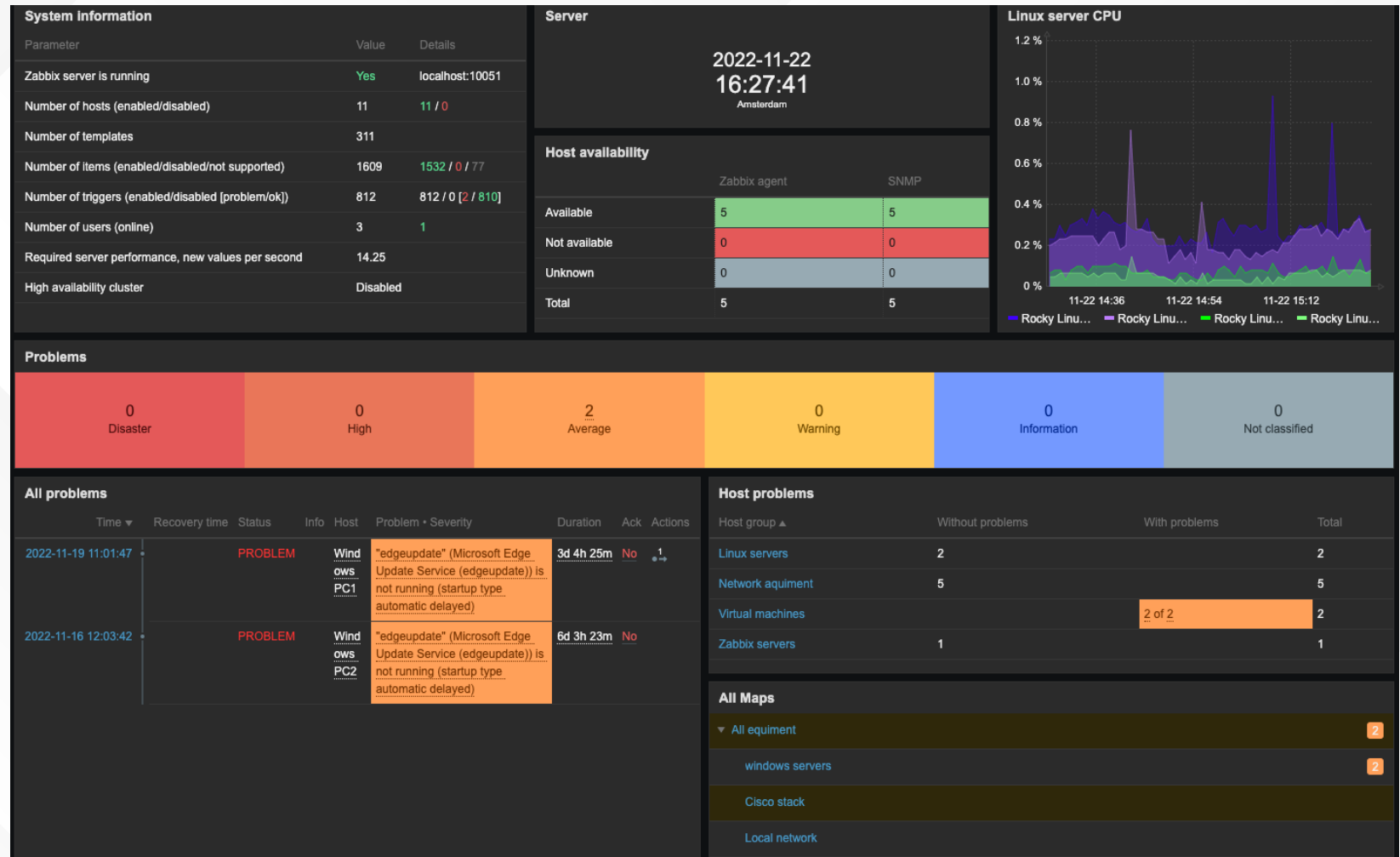
<https://blog.zabbix.com/tags-in-zabbix-6-0-lts-usage-subfilters-and-guidelines/19565/>

Info	Tags
	scope: availability scope: capacity
	scope: availability scope: capacity
	scope: capacity scope: performance
	scope: capacity scope: performance
	scope: availability scope: capacity
	scope: availability scope: capacity
	scope: capacity scope: performance
	scope: capacity scope: performance
	scope: security



# Dashboards/widgets

- What do you see?
- Is this practical?



# Frontend filters

- Options
- Named filter
- Main filters
- Sub filters

The screenshot shows the Zabbix frontend filter configuration page. At the top, there are search fields for 'Host groups', 'Hosts', and 'Name'. To the right, there are 'Tags' configuration options, including 'And/Or' logic, a tag input field, a dropdown for the operator (set to 'Contains'), a 'value' input field, and a 'Remove' button. Below these are options for 'Show tags' (None, 1, 2, 3), 'Tag name' (Full, Shortened, None), and 'Tag display priority' (comma-separated list). There are also 'Save as', 'Apply', and 'Reset' buttons.

The main content area is divided into sections:

- Subfilter**: affects only filtered data
- HOSTS**: [Windows client](#) 112, [Zabbix server](#) 125
- TAGS**: [component](#) 237, [description](#) 9, [disk](#) 16, [filesystem](#) 11, [interface](#) 18, [name](#) 51, [service](#) 51
- TAG VALUES**:
  - component**: [application](#) 2, [cpu](#) 25, [data-collector](#) 13, [environment](#) 1, [internal-process](#) 20, [memory](#) 19, [network](#) 18, [os](#) 6, [raw](#) 3, [security](#) 1, [storage](#) 43, [system](#) 93
  - description**: [Ethernet0](#) 9
  - disk**: [0 C:](#) 8, [sda](#) 8
  - filesystem**: [/](#) 4, [/boot](#) 4, [C:](#) 3
  - interface**: [ens192](#) 9, [Intel\(R\) 82574L Gigabit Network Connection](#) 9
  - name**: [Background Tasks Infrastructure Service](#) 1, [Base Filtering Engine](#) 1, [COM+ Event System](#) 1, [Connected User Experiences and Telemetry](#) 1, [CoreMessaging](#) 1, [Cryptographic Services](#) 1, [Data Usage](#) 1, [DCOM Server Process Launcher](#) 1, [DHCP Client](#) 1, [Diagnostic Policy Service](#) 1, [Display Policy Service](#) 1, [Distributed Link Tracking Client](#) 1, [DNS Client](#) 1, [IP Helper](#) 1, [Local Session Manager](#) 1, [Microsoft Defender Antivirus Service](#) 1, [Microsoft Edge Update Service \(edgeupdate\)](#) 1, [Network Location Awareness](#) 1, [Network Store Interface Service](#) 1, [Power](#) 1, [Print Spooler](#) 1, [Remote Procedure Call \(RPC\)](#) 1, [RPC Endpoint Mapper](#) 1, [Security Accounts Manager](#) 1, [Security Center](#) 1, [Server](#) 1, [Storage Service](#) 1, [SysMain](#) 1, [System Event Notification Service](#) 1, [System Events Broker](#) 1, [System Guard Runtime Monitor Broker](#) 1, [Task Scheduler](#) 1, [Themes](#) 1, [Update Orchestrator Service](#) 1, [User Manager](#) 1, [User Profile Service](#) 1, [VMware Alias Manager and Ticket Service](#) 1, [VMware SVGA Helper Service](#) 1, [VMware Tools](#) 1, [Windows Audio](#) 1, [Windows Audio Endpoint Builder](#) 1, [Windows Connection Manager](#) 1, [Windows Defender Firewall](#) 1, [Windows Event Log](#) 1, [Windows Font Cache Service](#) 1, [Windows Management Instrumentation](#) 1, [Windows Push Notifications System Service](#) 1, [Windows Search](#) 1, [Workstation](#) 1, [Zabbix Agent](#) 1, [Zabbix Agent 2](#) 1
  - service**: [AudioEndpointBuilder](#) 1, [Audiosrv](#) 1, [BFE](#) 1, [BrokerInfrastructure](#) 1, [CoreMessagingRegistrar](#) 1, [CryptSvc](#) 1, [DcomLaunch](#) 1, [Dhcp](#) 1, [DiagTrack](#) 1, [DispBrokerDesktopSvc](#) 1, [Dnscache](#) 1, [DPS](#) 1, [DusmSvc](#) 1, [edgeupdate](#) 1, [EventLog](#) 1, [EventSystem](#) 1, [FontCache](#) 1, [iphlpvc](#) 1, [LanmanServer](#) 1, [LanmanWorkstation](#) 1, [LSM](#) 1, [mpssvc](#) 1, [NlaSvc](#) 1, [nsi](#) 1, [Power](#) 1, [ProfSvc](#) 1, [RpcEptMapper](#) 1, [RpcSs](#) 1, [SamSs](#) 1, [Schedule](#) 1, [SENS](#) 1, [SgrmBroker](#) 1, [Spooler](#) 1, [StorSvc](#) 1, [SysMain](#) 1, [SystemEventsBroker](#) 1, [Themes](#) 1, [TrkWks](#) 1, [UserManager](#) 1, [UsSvc](#) 1, [VGAAuthService](#) 1, [vm3dservice](#) 1, [VMTools](#) 1, [WcmSvc](#) 1, [WinDefend](#) 1, [Winmgmt](#) 1, [WpnService](#) 1, [wscsv](#) 1, [WSearch](#) 1, [Zabbix Agent](#) 1, [Zabbix Agent 2](#) 1

At the bottom, there is a 'DATA' section with 'With data' and 'Without data' options.

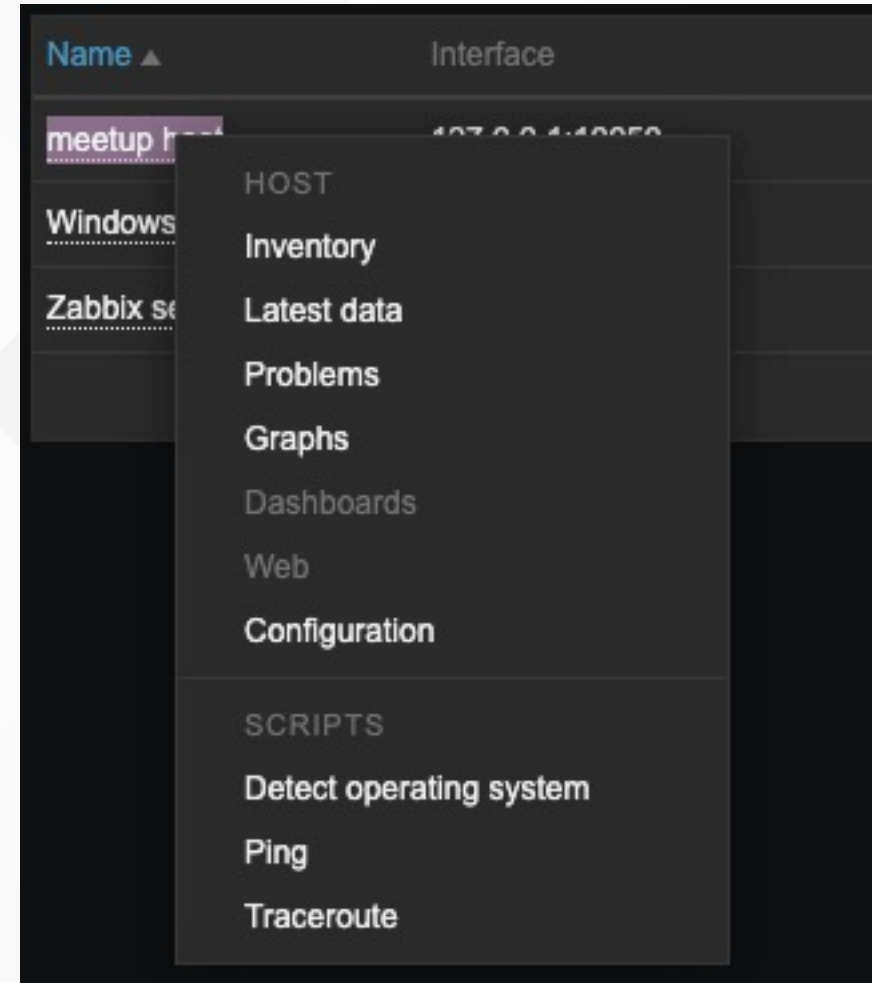
# Doing more with problems

- How?
- Frontend scripts
- Urls
- Historical data





- What are they?
- What types can you use?
- How can you use them?



# Trigger URLs

- **Why** would you use them?
- **How** would you use them?

PROBLEM	Windows client	C:\share\temp_stuff\*.png: Is older than 15 minutes	34s	No
PROBLEM	Windows client 5.2	Zabbix agent is not available (for 3m) ?		

TRIGGER

- Problems
- Configuration

LINKS

- Trigger URL

HISTORY

- C:\share\temp\_stuff\\*.png: Time access

Allow manual close

URL

Description

Allow manual close

URL

Description

Allow manual close

URL

Allow manual close

URL

- How would you utilize this?
- Predictions
  - More info about Predictions? <https://support.zabbix.com/browse/ZBX-19043>
- Certain triggers
- Keep the history

Timestamp	System contact details
2022-11-25 14:18:18	me right@here.com
2022-11-25 14:17:18	me right@here.com
2022-11-25 14:16:18	me looking@you.com
2022-11-25 14:15:18	me looking@you.com
2022-11-25 14:14:18	me looking@you.com
2022-11-25 14:13:18	me looking@you.com
2022-11-25 14:12:18	me right@here.com
2022-11-25 14:11:18	me right@here.com
2022-11-25 14:10:18	me right@here.com
2022-11-25 14:09:18	me right@here.com
2022-11-25 14:08:18	me right@here.com
2022-11-25 14:07:18	me right@here.com
2022-11-25 14:06:18	me right@here.com
2022-11-25 14:00:18	me right@here.com



# What else?

- Is there more?
- What do I find handy?



Lets see if there are any questions in Q&A

