

# Opensource ICT Solutions

## ZABBIX ~~WEBINARS~~ MEETUP

Setting up items, triggers and LLD efficiently  
within Zabbix templates

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

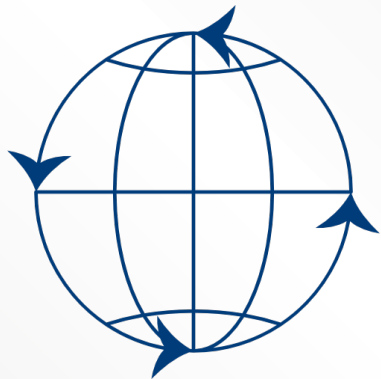


# Whoami



**Brian van Baekel**

Zabbix trainer / Consultant



**OpenSource ICT Solutions**

Your Zabbix partner in:

- The Netherlands
- United Kingdom
- United States



# What are templates?

- Blueprint of your monitoring needs
- Can consist out of
  - Items
  - Triggers
  - Graphs
  - LLD rules
  - Web monitoring
  - Dashboards



# But that's the same as on hosts!

- Almost the same settings/properties as on the host

## Template

<input type="checkbox"/> Name ▲	Hosts	Items	Triggers	Graphs	Dashboards	Discovery	Web	Linked templates	Linked to templates
<input type="checkbox"/> AIX by Zabbix agent	Hosts	Items 43	Triggers 10	Graphs 4	Dashboards 1	Discovery 2	Web		
<input type="checkbox"/> Alcatel Timetra TIMOS SNMP	Hosts	Items 19	Triggers 9	Graphs 3	Dashboards 1	Discovery 6	Web		
<input type="checkbox"/> Apache ActiveMQ by JMX	Hosts	Items	Triggers	Graphs	Dashboards	Discovery 2	Web		
<input type="checkbox"/> Apache by HTTP	Hosts	Items 22	Triggers 5	Graphs 3	Dashboards 1	Discovery 1	Web		

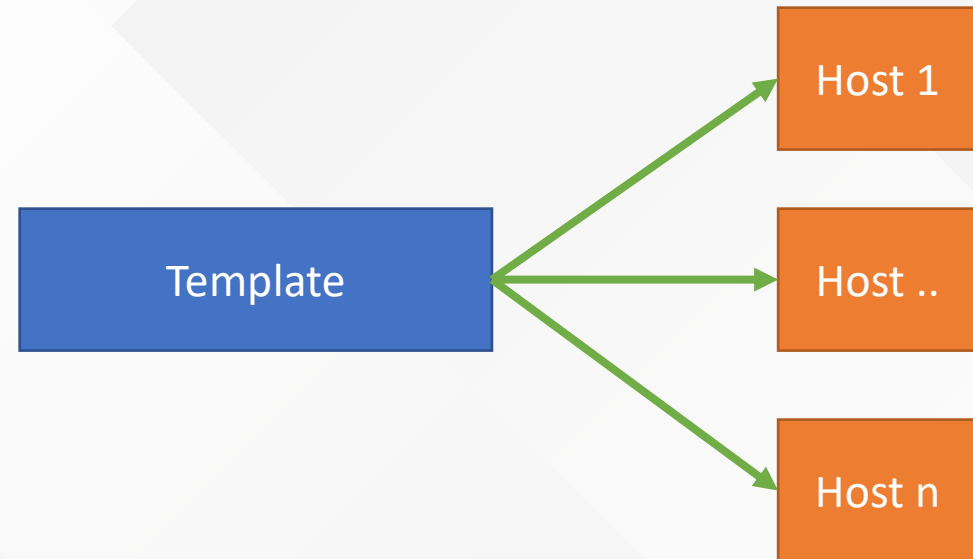
## Host

<input type="checkbox"/> Name ▲	Items	Triggers	Graphs	Discovery	Web	Interface	Proxy	Templates
<input type="checkbox"/> Zabbix server	Items 100	Triggers 56	Graphs 19	Discovery 5	Web	127.0.0.1:10050		Linux by Zabbix agent, Zabbix server health



# Should we use them?

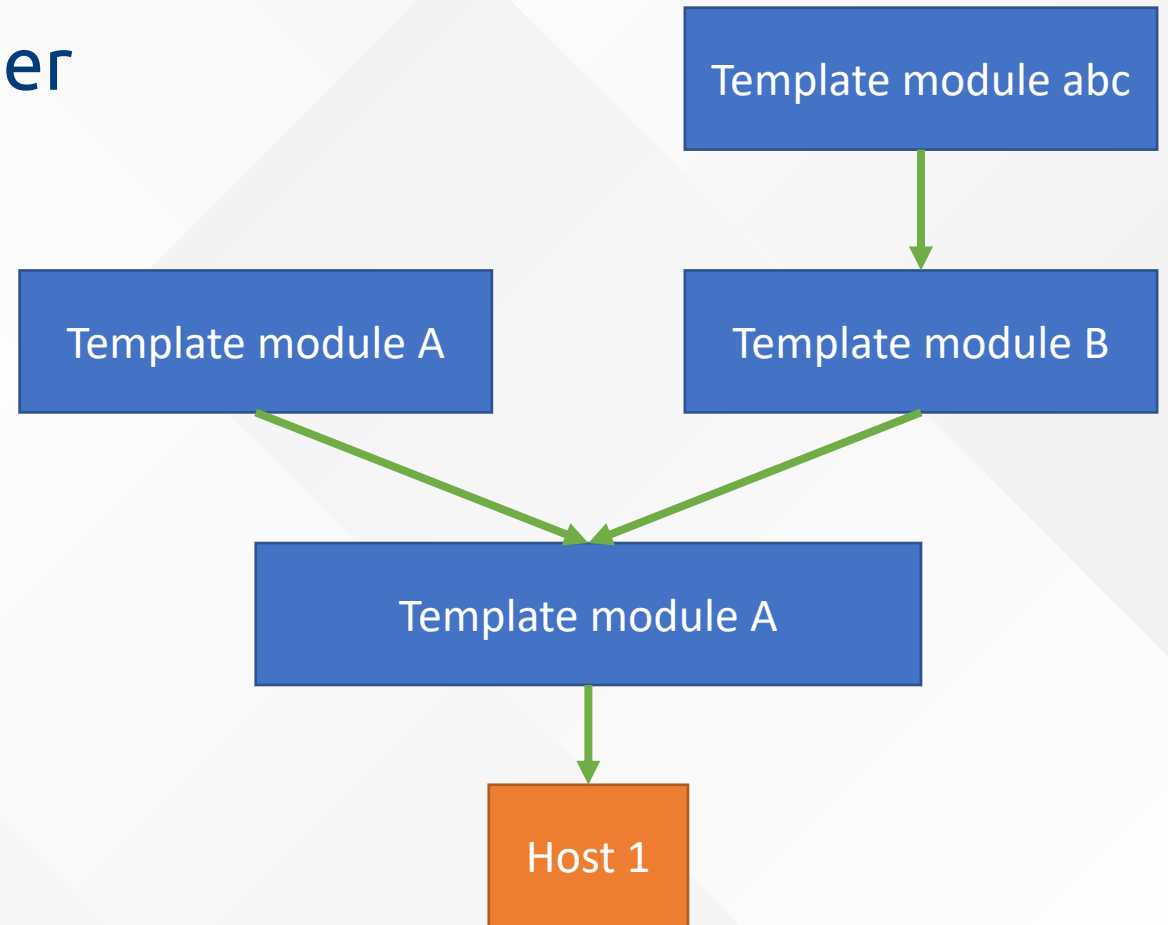
- YES.
- Templates are great for:
  - Quickly adding entities to hosts
  - Efficient mass updates
  - Config exports
  - Dynamic configurations



# Nested templates!

- We can link templates to each other

- Drawbacks:
  - Exporting them
  - Visibility
  - Versioning
  - ZBXNEXT-8087



# Naming

<input type="checkbox"/>	Linux by Zabbix agent	class: os	target: linux
<input type="checkbox"/>	Linux by Zabbix agent active	class: os	target: linux
<input type="checkbox"/>	Linux SNMP	class: os	target: linux

What      How

Type indicator  
now as tags

# Linking them

## Configuration -> Hosts

**New host**

Host IPMI Tags Macros Inventory Encryption Value mapping

\* Host name

Visible name

Templates

\* Host groups

- Linux filesystems SNMP
- Linux filesystems by Zabbix agent
- Windows filesystems by Zabbix agent
- Linux filesystems by Zabbix agent active
- Windows filesystems by Zabbix agent active

Interfaces

- Systemd by Zabbix agent 2
- Template module B
- Template module A

Description

visible name

Templates

\* Host groups

Interfaces No interfaces are defined.

[Add](#)

Description

**Mass update** ? x

Host IPMI Tags Macros Inventory Encryption Value mapping

Link templates

Clear when unlinking

Host groups  Original

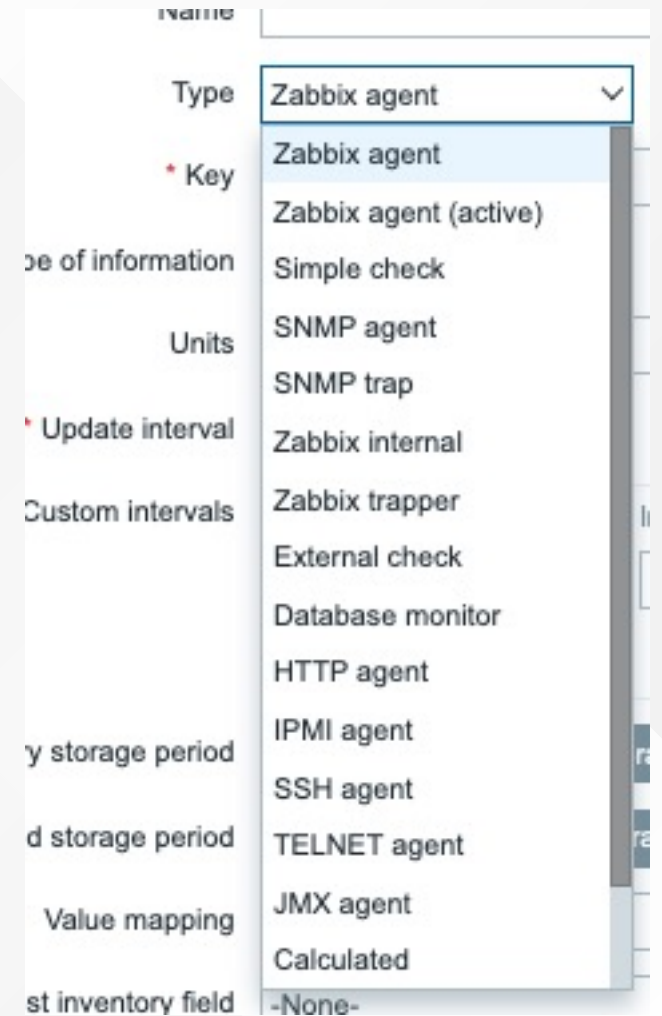
Description  Original

Monitored by proxy  Original

Status  Original



- Metrics
- Various types supported:



# Built direct or on templates?

- Items can be created on hosts directly
- But also on templates
  
- Pick one, but do NOT mix and match



# Making them dynamic -> macros

- We want to check SSH availability, via an item on a template:

Preprocessing

* Name	<input type="text"/>	* Name	<input type="text"/>
Type	Simple check ▾	Type	Simple check ▾
* Key	net.tcp.service[service,<ip>,<port>] <input type="button" value="Select"/>	* Key	net.tcp.service[ssh,,] <input type="button" value="Select"/>

- But what if we must check a non default port?

* Name	<input type="text"/>
Type	Simple check ▾
* Key	net.tcp.service[ssh,,2222] <input type="button" value="Select"/>

- But only one please...

* Name	<input type="text"/>
Type	Simple check ▾
* Key	net.tcp.service[ssh,,{SSH.PORT}] <input type="button" value="Select"/>

# Overriding macros

- Define default value on template level

All templates / Template module A | Items | Triggers | Graphs | Dashboards | Discovery rules | Web scenarios

Templates | Tags | **Macros 1** | Value mapping

Template macros | Inherited and template macros

Macro	Value	Description
{SSH.PORT}	22	My default SSH port macro

[Add](#)

[Update](#) [Clone](#) [Full clone](#) [Delete](#) [Delete and clear](#) [Cancel](#)

New host

Host | IPMI | Tags | **Macros** | Inventory | Encryption | Value mapping

Host macros | Inherited and host macros

Macro	Effective value	Template value
{SNMP_COMMUNITY}	public	
description		
{SSH.PORT}	22	Template module A: "22"
My default SSH port macro		

[Add](#)

New host

Host | IPMI | Tags | **Macros 1** | Inventory | Encryption | Value mapping

Host macros | Inherited and host macros

Macro	Effective value	Template value
{SNMP_COMMUNITY}	public	
description		
{SSH.PORT}	2222	Template module A: "22"
My default SSH port macro		

[Add](#)

# Update your items

- Changes made on templates, will be propagated to items on hosts. Immediately!

Items

All hosts / Zabbix server Enabled ZBX Items 100 Triggers 56 Graphs 19 Discovery rules 5 Web scenarios

Item Tags 1 Preprocessing

Parent items [Linux by Zabbix agent](#)

\* Name Available memory

Type Zabbix agent

\* Key vm.memory.size[available]

Type of information Numeric (unsigned)

\* Host interface 127.0.0.1:10050

Units B

\* Update interval 1m



- Problem definition
- Default state: OK
- If problem is detected, it will switch to PROBLEM state
- On each state change events are generated

### Triggers

All templates / Template module A Items **Triggers** Graphs Dashboards Discovery rules Web scenarios

Trigger **Tags** Dependencies

\* Name

Event name

Operational data

Severity

\* Expression

[Expression constructor](#)

OK event generation

PROBLEM event generation mode

OK event closes

Allow manual close

Menu entry name

Menu entry URL


Description

Enabled


# Naming

- What is wrong?

**Average** Zabbix agent is not available  
(for {AGENT.TIMEOUT})




**Average** The Zabbix agent has been unavailable for 5  
minutes on {HOST.HOST}




- Where did it go wrong?

Time	Severity	Recovery time	Status	Info	Host	Problem	Duration	Ack	Actions	Tags
10:16:09	<input type="checkbox"/> Average		PROBLEM		summit-linux-02	Zabbix agent is not available (for 3m) ?	30s	No	1	class: os component: system scope: availability ...



Time	Severity	Recovery time	Status	Info	Host	Problem	Duration	Ack	Actions	Tags
10:24:09	<input type="checkbox"/> Average		PROBLEM		summit-linux-02	The Zabbix agent has been unavailable for 5 minutes on summit-linux-02 ?	46s	No	1	class: os component: system scope: availability ...



- How am I fixing it?



- If the last value that came is, is above 5, go into problem state

* Name	<input type="text" value="CPU load is too high (&gt;5)"/>
Event name	<input type="text" value="CPU load is too high (&gt;5)"/>
Operational data	<input type="text"/>
Severity	<input type="button" value="Not classified"/> <input type="button" value="Information"/> <input type="button" value="Warning"/> <input checked="" type="button" value="Average"/> <input type="button" value="High"/> <input type="button" value="Disaster"/>
* Expression	<input type="text" value="last(/Template module A/system.cpu.load)&gt;5"/> <input type="button" value="Add"/>



- Change static threshold to macros!

\* Name

Event name

Operational data

Severity

\* Expression

\* Name

Event name

Operational data

Severity

\* Expression

Macro	Value	Description
<input type="text" value="{SSH.PORT}"/>	<input type="text" value="22"/>	<input type="text" value="My default SSH port macro"/> <a href="#">Remove</a>
<input type="text" value="{CPU.LOAD.HIGH}"/>	<input type="text" value="5"/>	<input type="text" value="description"/> <a href="#">Remove</a>

[Add](#)

- Monitoring → Problems

<input type="checkbox"/>	Time ▾	Severity	Recovery time	Status	Info	Host	Problem	Duration	Ack	Actions	Tags
<input type="checkbox"/>	19:13:12	Average		PROBLEM		host	CPU load is too high (1)	1m 10s	No		

Displaying 1 of 1 found

Show operational data

None  Separately  With problem name

<input type="checkbox"/>	Time ▾	Severity	Recovery time	Status	Info	Host	Problem	Operational data	Duration	Ack	Actions	Tags
<input type="checkbox"/>	19:13:12	Average		PROBLEM		host	CPU load is too high (1)	1.94	2m 7s	No		

Displaying 1 of 1 found

- Trigger configuration

\* Name

Event name

Operational data

Severity Not classified Information Warning Average High Disaster

\* Expression

- Problem name

<input type="checkbox"/>	Time ▼	Severity	Recovery time	Status	Info	Host	Problem	Operational data	Duration	Ack	Actions	Tags
<input type="checkbox"/>	19:13:12	Average		PROBLEM		host	CPU load is too high (1)	Current CPU load is: 2.04	4m 39s	No		

Displaying 1 of 1 found

- But.... What is the average increase in the last X period?

\* Name

Event name

Operational data

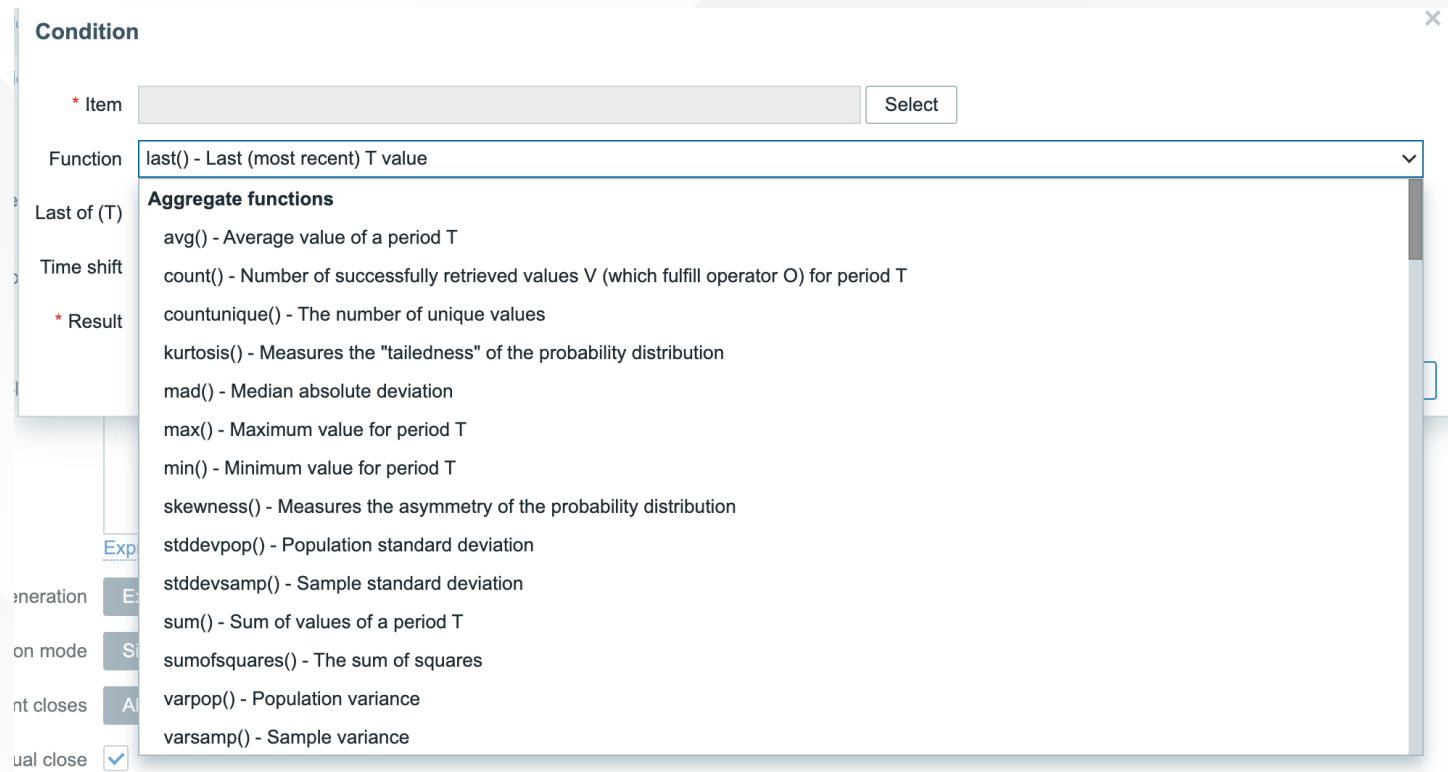
Severity

\* Expression

<input type="checkbox"/>	Time ▾	Severity	Info	Host	Problem	Operational data	Duration	Ack	Actions	Tags
<input type="checkbox"/>	19:29:32	Average		host	Load increased by 174% in the last 15 minutes.	Current CPU load is: 2.11	1s	No		

Displaying 1 of 1 found

- Last function is often not the best idea
- Full list is in the docs (and it's extensive)



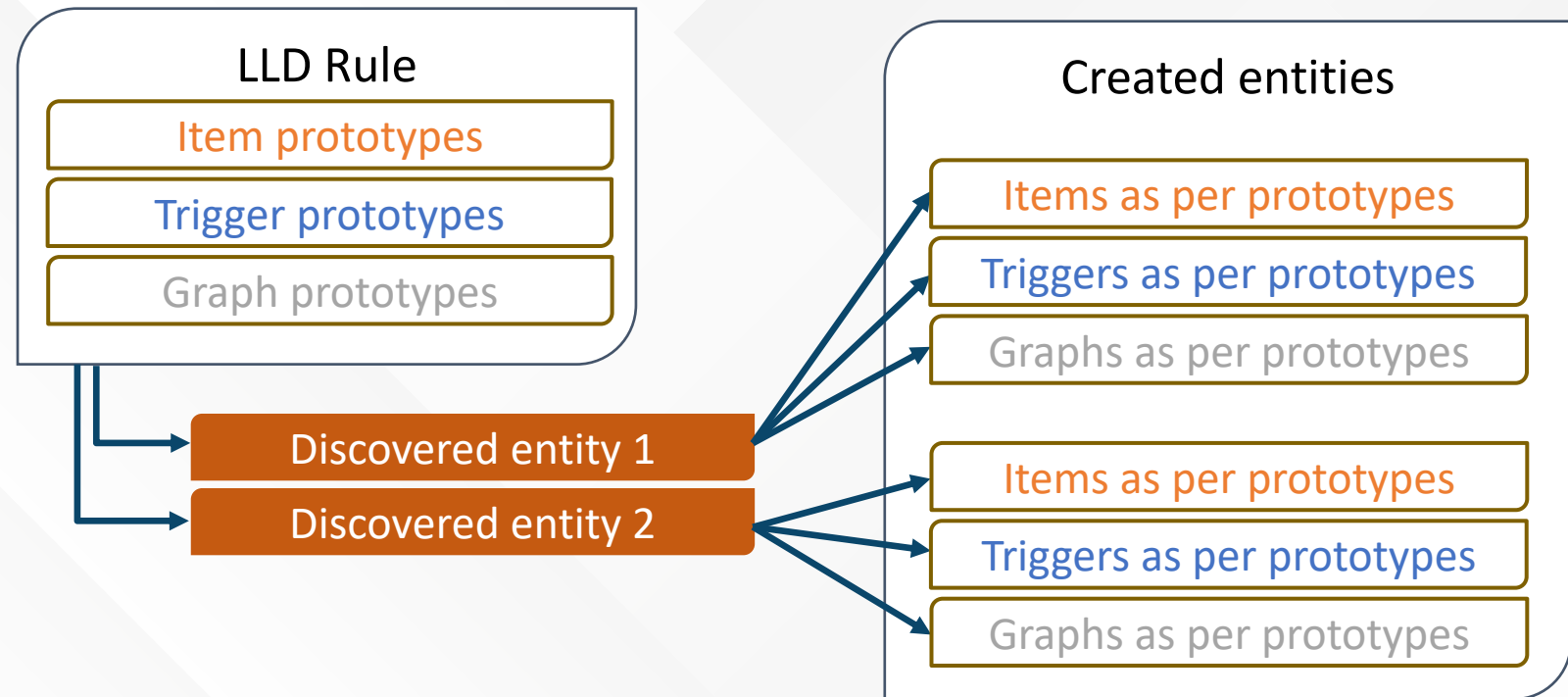
The screenshot shows a software interface with a 'Condition' window. The window has a title bar with a close button (X). Below the title bar, there is a field labeled '\* Item' with a 'Select' button to its right. Below that, there is a dropdown menu labeled 'Function' with the text 'last() - Last (most recent) T value' and a downward arrow. Below the dropdown, there is a list of functions under the heading 'Aggregate functions'. The list includes: 'avg() - Average value of a period T', 'count() - Number of successfully retrieved values V (which fulfill operator O) for period T', 'countunique() - The number of unique values', 'kurtosis() - Measures the "tailedness" of the probability distribution', 'mad() - Median absolute deviation', 'max() - Maximum value for period T', 'min() - Minimum value for period T', 'skewness() - Measures the asymmetry of the probability distribution', 'stddevpop() - Population standard deviation', 'stddevsamp() - Sample standard deviation', 'sum() - Sum of values of a period T', 'sumofsquares() - The sum of squares', 'varpop() - Population variance', and 'varsamp() - Sample variance'. On the left side of the window, there are several labels: 'Last of (T)', 'Time shift', and '\* Result'. At the bottom left of the window, there are several labels: 'eneration', 'on mode', 'nt closes', and 'ual close', each with a corresponding button or checkbox.



- A way to automatically create:
  - Items
  - Triggers
  - Graphs
  - Host dashboards
  - Hosts
- Once an entity is added, Zabbix will detect it.
- Once an entity is removed, Zabbix can clean it up



- Create discovery rule
- Define prototypes (of items, triggers etc)



# Discovery rule

- Can be created on template or host level

Discovery rules

All templates / Linux by Zabbix agent / Discovery list / Mounted filesystem discovery / Item prototypes 4 / Trigger prototypes 4 / Graph prototypes 1 / Hosts 1

Discovery rule Preprocessing LLD macros Filters 4 Overrides

\* Name

Type

\* Key

\* Update interval

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

[Add](#)

\* Keep lost resources period

Description

Enabled

- Type
- \* Key
- Zabbix agent (active)
- Simple check
- SNMP agent
- Zabbix internal
- Zabbix trapper
- External check
- Database monitor
- HTTP agent
- IPMI agent
- SSH agent
- TELNET agent
- JMX agent
- Dependent item
- Script



# Discovery rule 2

- Works with JSON data
- With Preprocessing and LLD macros you can change 'not correct' data into something Zabbix understands
- Low Level Discovery macros are key.  
Format: {#MACRO}

```
[  
  {  
    "{#FSNAME}":"/sys",  
    "{#FSTYPE}":"sysfs"  
  },  
  {  
    "{#FSNAME}":"/boot",  
    "{#FSTYPE}":"xfs"  
  },  
  {  
    "{#FSNAME}":"/dev",  
    "{#FSTYPE}":"devtmpfs"  
  },  
]
```



# Item prototype

## Item prototypes

All templates / Linux by Zabbix agent / Discovery list / Mounted filesystem discovery / Item prototypes 4 / Trigger prototypes 4 / Graph prototypes 1 / Host prototypes

Item prototype Tags 2 Preprocessing

\* Name

Type

\* Key

Type of information

Units

\* Update interval

Type	Interval	Period	Action
<input type="button" value="Flexible"/> <input type="button" value="Scheduling"/>	<input type="text" value="50s"/>	<input type="text" value="1-7,00:00-24:00"/>	<input type="button" value="Remove"/>

\* History storage period

\* Trend storage period

Value mapping

Description

Create enabled

Discover



Discovered by **Mounted filesystem discovery**

\* Name

Type

\* Key

Type of information

\* Host interface

Units

\* Update interval

Type	Interval	Period
<input type="button" value="Flexible"/> <input type="button" value="Scheduling"/>	<input type="text" value="50s"/>	<input type="text" value="1-7,00:00-24:00"/>

History storage period

\* Trend storage period

Value mapping

Description



# Trigger prototype

\* Name

Event name %})"/>

Operational data

Severity

\* Expression

Expression constructor

<input type="checkbox"/>	Time ▾	Severity	Info	Host	Problem	Duration	Ack	Actions	Tags
<input type="checkbox"/>	12:17:36	Warning		Zabbix server	↓ /boot: Disk space is low (used > 5%) ?	1m 9s	No		class: os component: storage filesystem: /boot ...

- By default, ALL discovered entities will be added
- This might be NOT what you want, because a lot of 'useless' information might come in
- Filters are **one** way of fixing this:

All templates / Linux by Zabbix agent / Discovery list / Mounted filesystem discovery / Item prototypes 4 / Trigger prototypes 4 / Graph prototypes 1 / Host prototypes

Discovery rule / Preprocessing / LLD macros / **Filters 1** / Overrides

Filters	Label	Macro	Regular expression	Action
A	{#FSTYPE}	matches	^(xfs sysfs)\$	<a href="#">Remove</a>

[Add](#)

[Update](#) [Clone](#) [Test](#) [Delete](#) [Cancel](#)



# Override - filter

**Override** ✕

\* Name

If filter matches

Filters

Label	Macro		Regular expression	Action
A	<input type="text" value="{#MACRO}"/>	matches	<input type="text" value="regular expression"/>	<a href="#">Remove</a>

[Add](#)

Operations

Condition

[Add](#)

# Override - filter

**Override** ✕

\* Name

If filter matches

Filters	Label	Macro		Regular expression	Action
	A	<input type="text" value="{#FSTYPE}"/>	matches	<input type="text" value="^(?!xfs ssyfs).*\$"/>	<a href="#">Remove</a>

[Add](#)

**New operation** ✕

Object

Condition

Create enabled  Original

Discover

Update interval  Original

History storage period  Original

Trend storage period  Original

Tags  Original

# Override per item match

- Overrides are extremely flexible

**Override** [Close]

Name: XFS important

If filter matches: **Continue overrides** Stop processing

Label	Macro	Regular expression	Action
A	{#FSTYPE}	matches ^{(xfs)\$	<a href="#">Remove</a>

[Add](#)

Operations

Condition	Action
Item prototype matches .*	<a href="#">Edit</a> <a href="#">Remove</a>
Trigger prototype matches .*	<a href="#">Edit</a> <a href="#">Remove</a>

[Add](#) [Cancel](#)

**New operation**

Object: Item prototype

Condition: matches .\*

Create enabled  Original

Discover  Original

Update interval  Delay 10s

Custom intervals: 

Type	Interval	Period	Action

[Add](#)

**New operation** [Close]

Object: Trigger prototype

Condition: matches .\*

Create enabled  Original

Discover  Original

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

Tags  Original

[Add](#) [Cancel](#)

# Combinations are possible

- Filters to get only the needed items
  - Only add physical filesystems
- Overrides to change behaviour
  - But /home is never important enough to trigger a 24/7 escalations





- This was just a high level overview / introduction to items, triggers and Low Level Discovery rules
- Each topic can takes hours (or even days) to explain in depth



Lets see if there are any questions in Q&A

