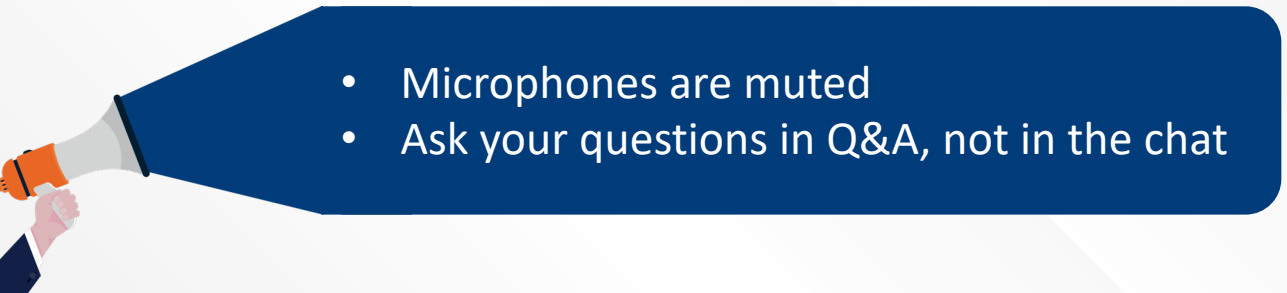
Opensource ICT Solutions

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

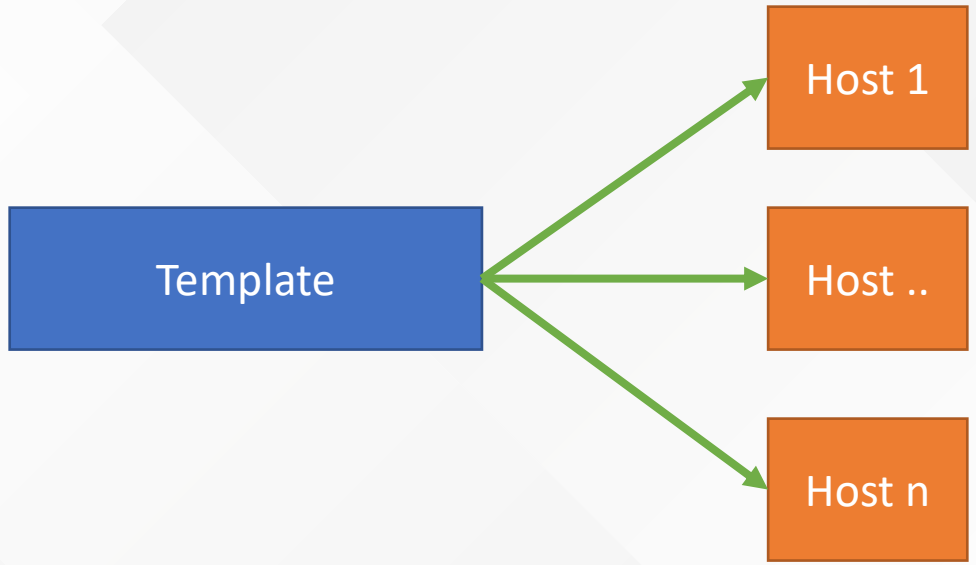
Name ▲	Hosts	Items	Triggers	Graphs	Dashboards	Discovery	Web	Linked templates	Linked to templates
AIX by Zabbix agent	Hosts	Items 43	Triggers 10	Graphs 4	Dashboards 1	Discovery 2	Web		
Alcatel Timetra TiMOS SNMP	Hosts	Items 19	Triggers 9	Graphs 3	Dashboards 1	Discovery 6	Web		
Apache ActiveMQ by JMX	Hosts	Items	Triggers	Graphs	Dashboards	Discovery 2	Web		
Apache by HTTP	Hosts	Items 22	Triggers 5	Graphs 3	Dashboards 1	Discovery 1	Web		

Host

Name ▲	Items	Triggers	Graphs	Discovery	Web	Interface	Proxy	Templates
Zabbix server	Items 100	Triggers 56	Graphs 19	Discovery 5	Web	127.0.0.1:10050		Linux by Zabbix agent, Zabbix server health

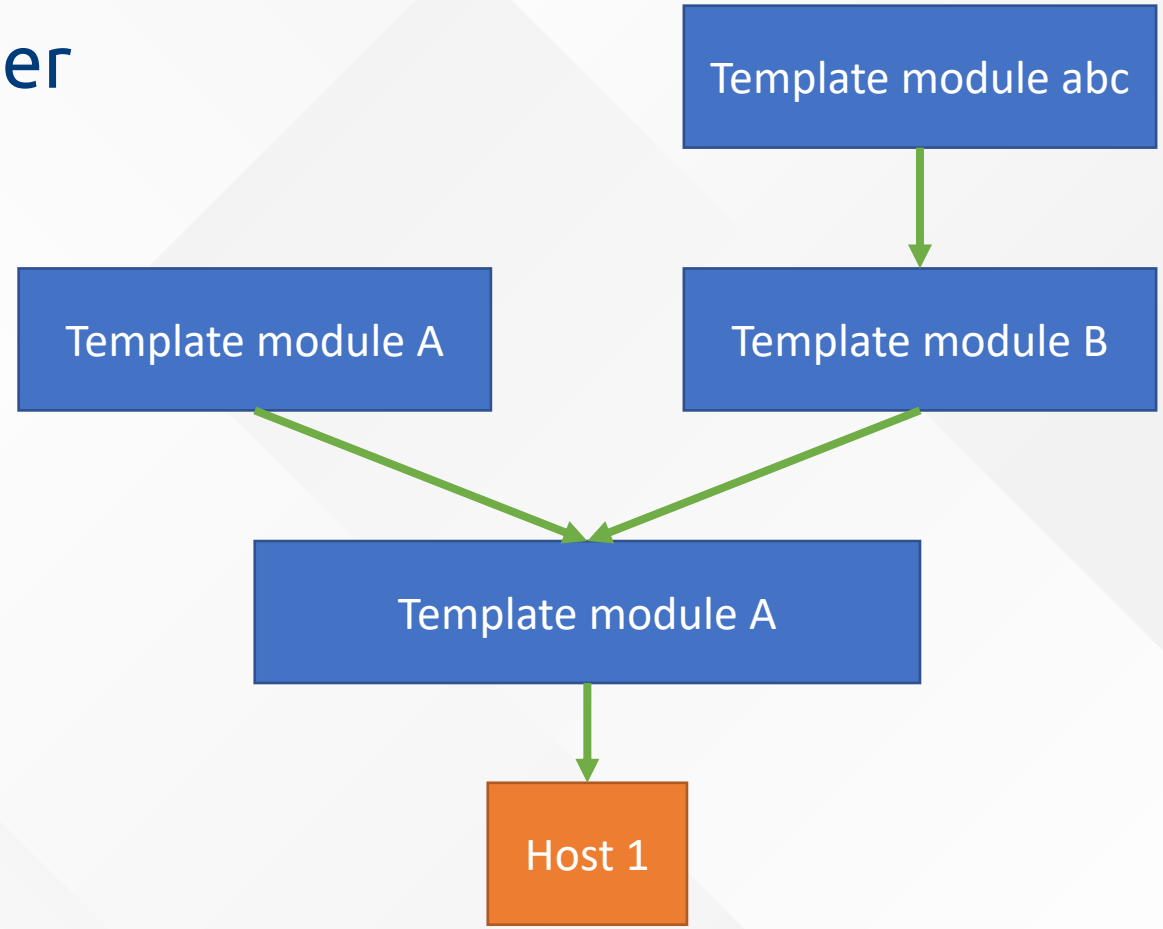
Should we use them?

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



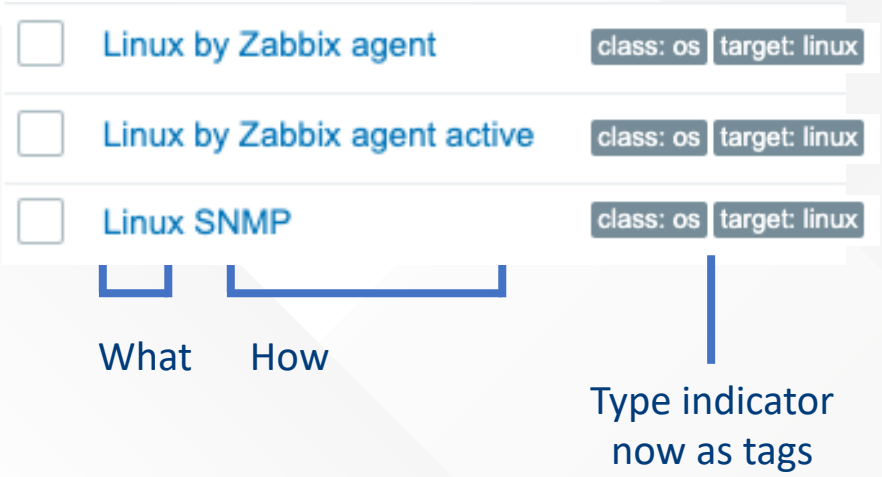
Nested templates!

- We can link templates to eachother



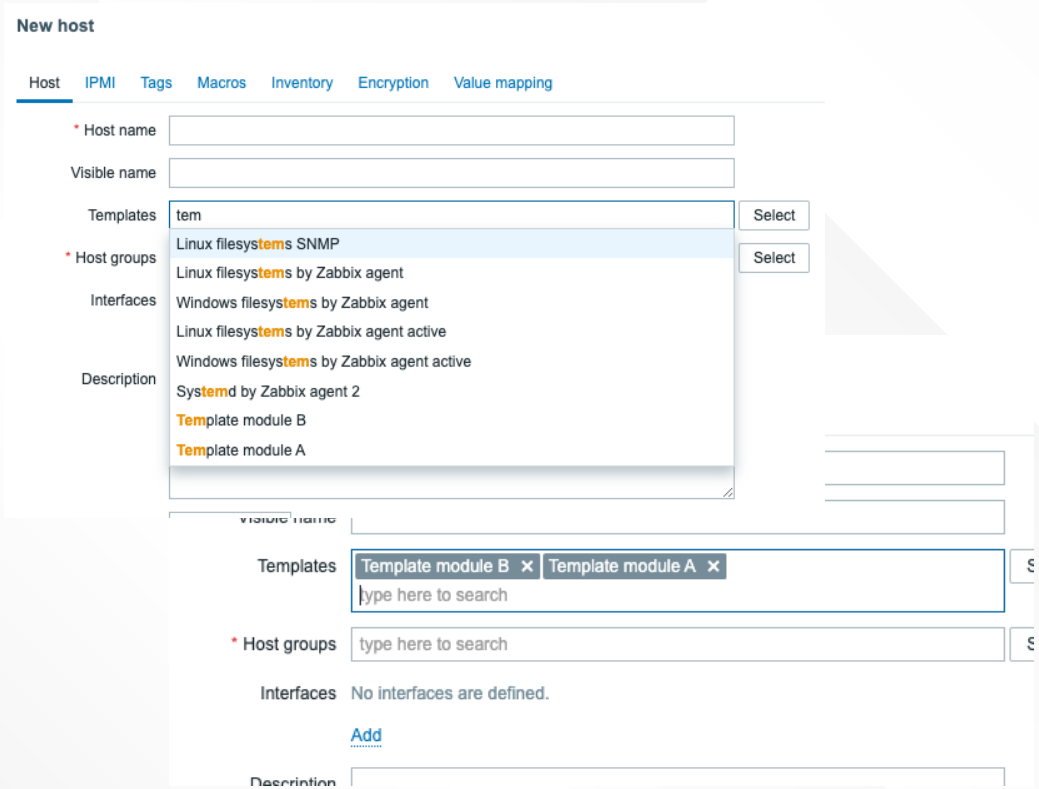
- Drawbacks:
  - Exporting them
  - Visibility
  - Versioning
  - ZBXNEXT-8087

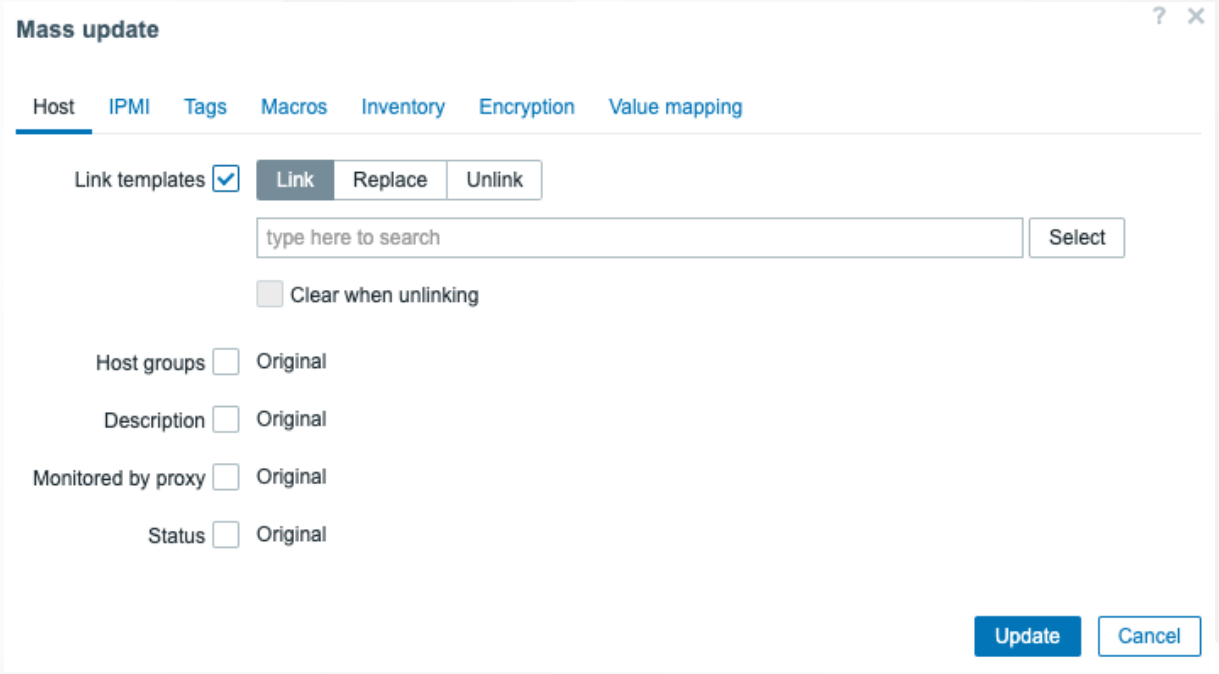
Naming


Linux by Zabbix agent
class: os
target: linux
Linux by Zabbix agent active
class: os
target: linux
Linux SNMP
class: os
target: linux
What
How
Type indicator
now as tags

Linking them

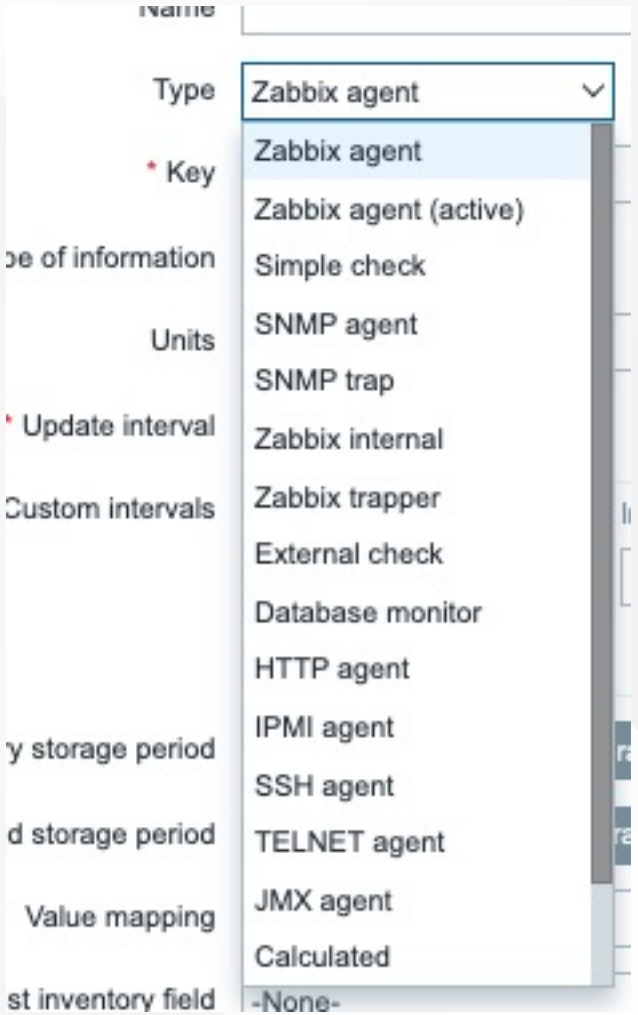
Configuration -> Hosts





Items

- Metrics
- Various types supported:



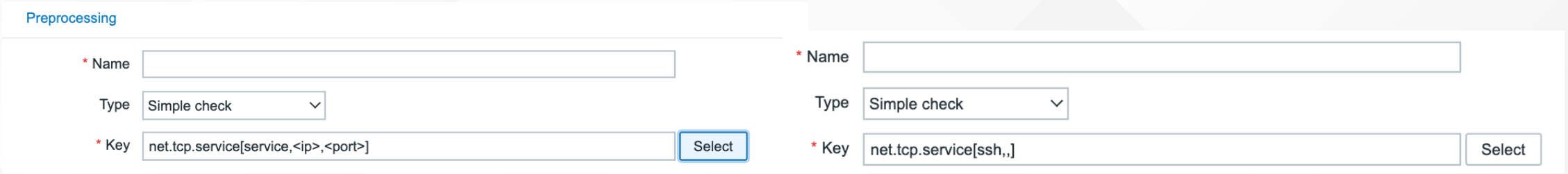
Built direct or on templates?

- Items can be created on hosts directly
- But also on templates

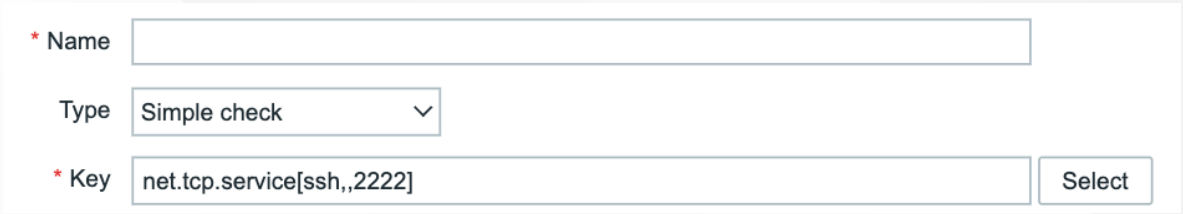
- Pick one, but do NOT mix and match

Making them dynamic -> macros

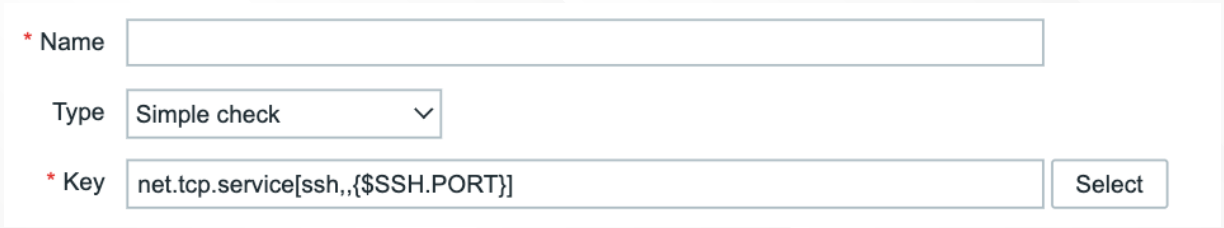
- We want to check SSH availability, via an item on a template:



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

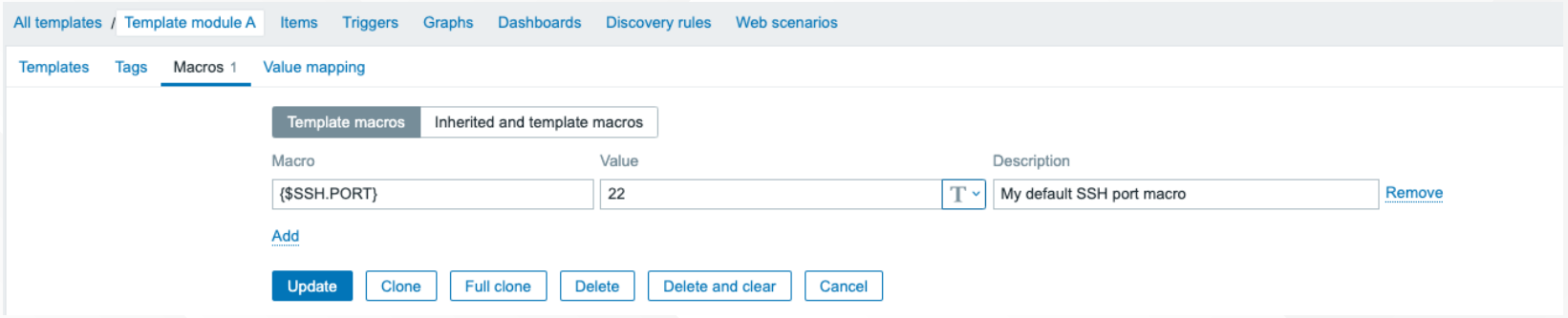


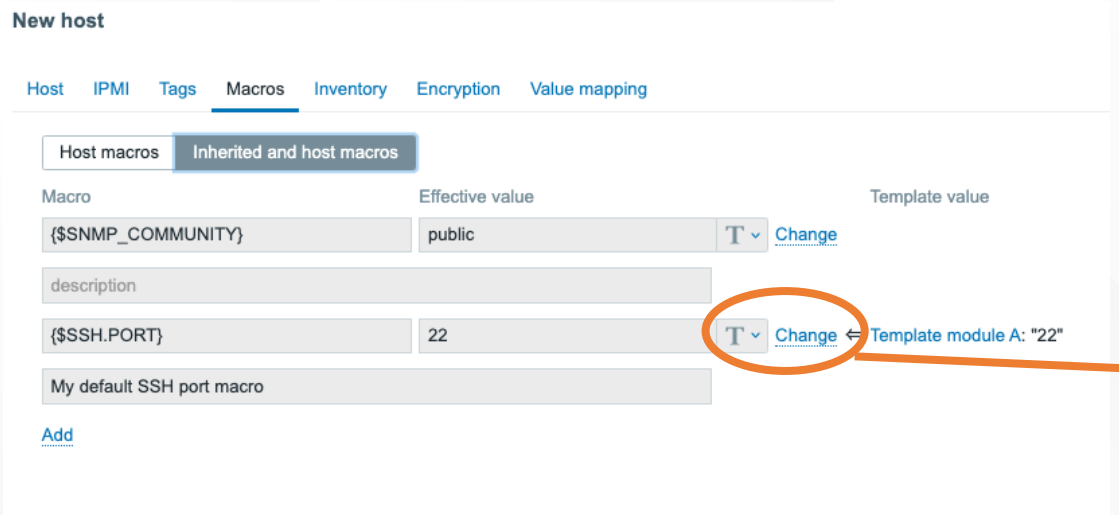
- But only one please…

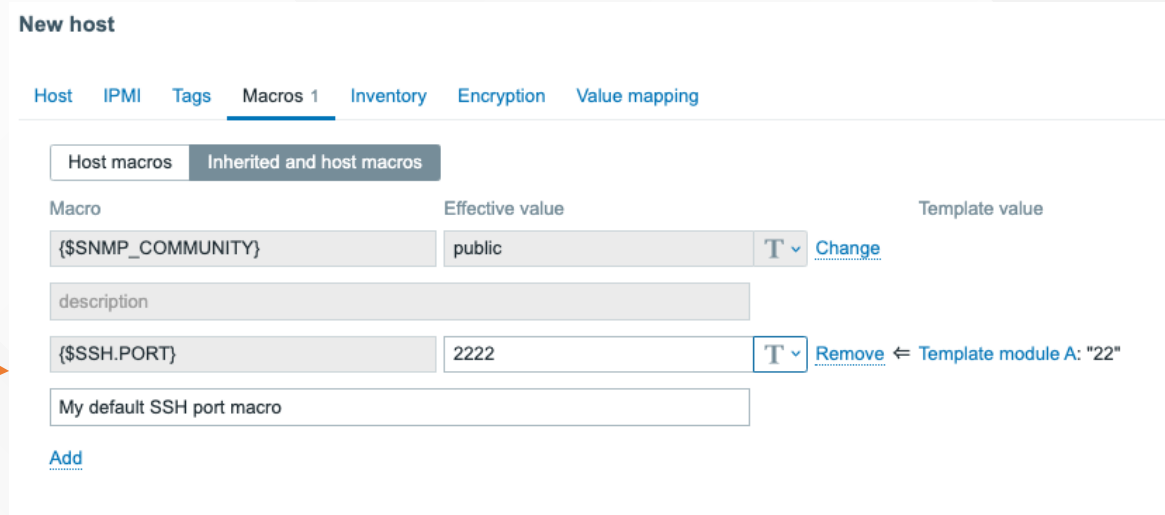


Overriding macros

- Define default value on template level

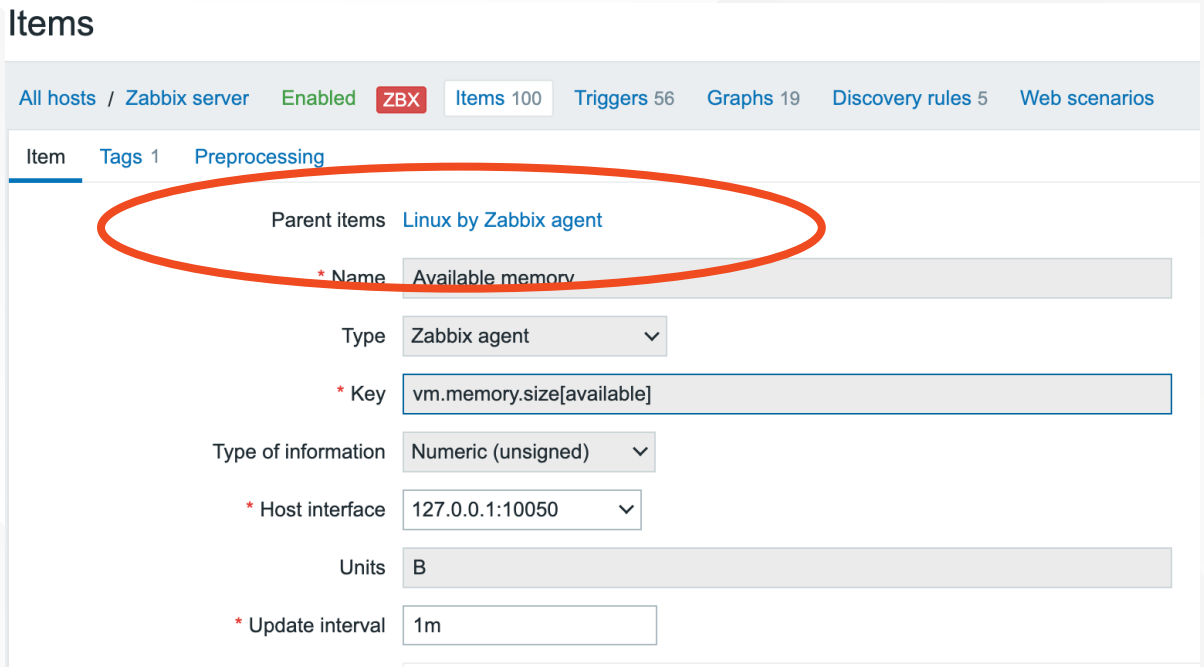






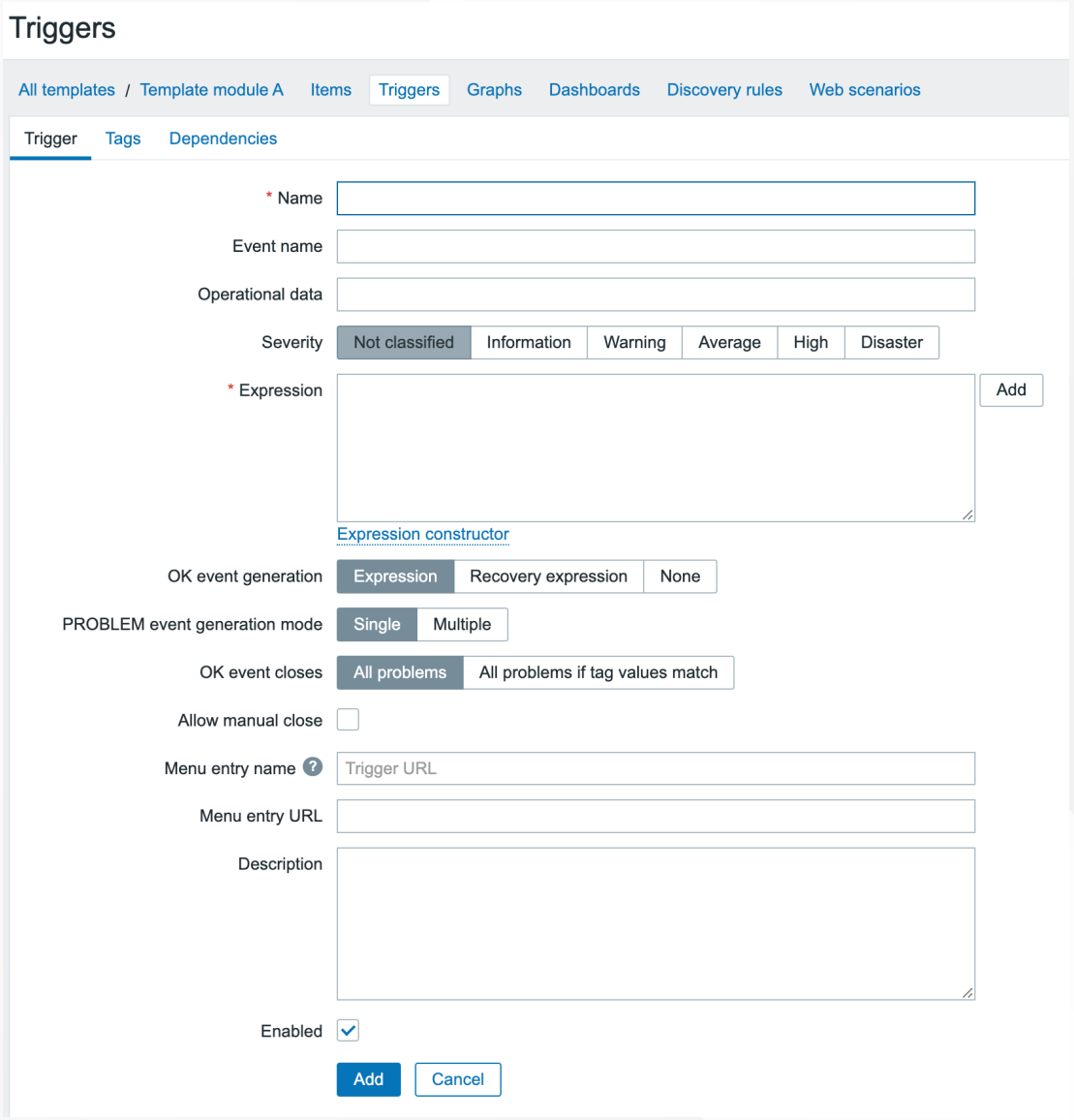
Update your items

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



Triggers

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



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?

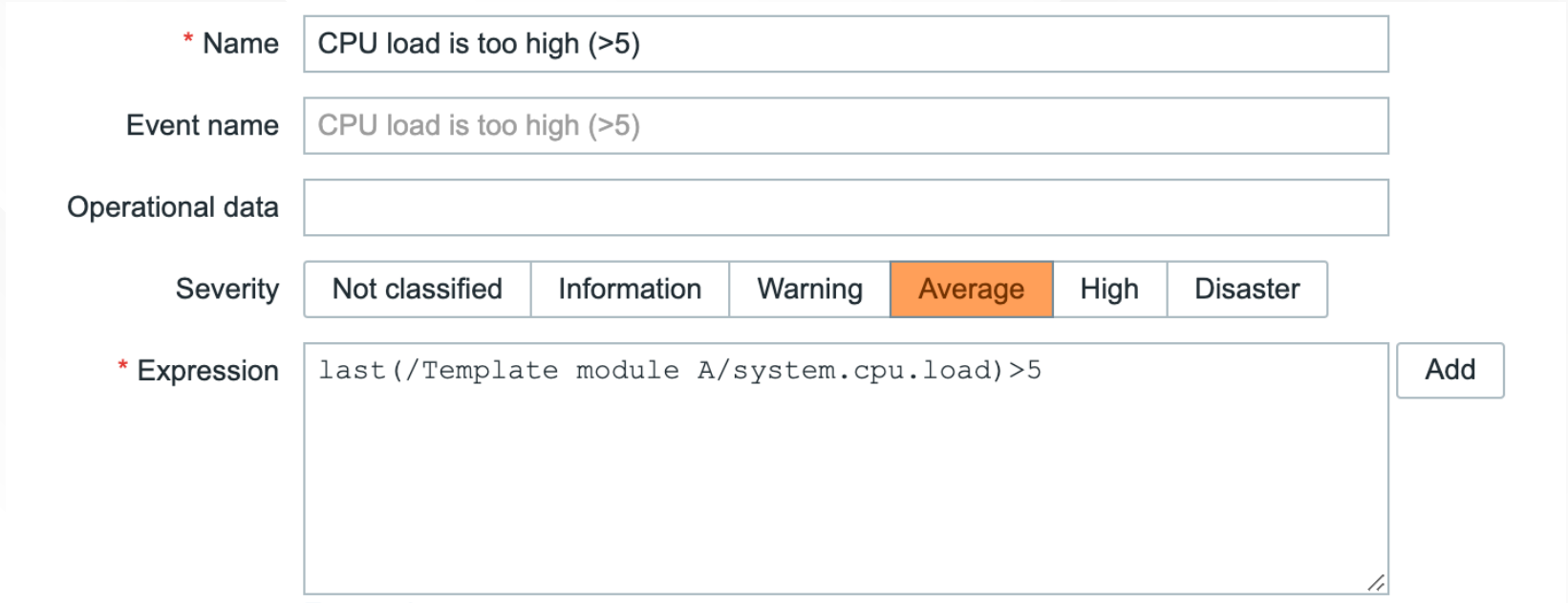
Time ▾	☐	Severity	Recovery time	Status	Info	Host	Problem	Duration	Ack	Actions	Tags
10:16:09	☐	Average		PROBLEM		summit-linux-02	Zabbix agent is not available (for 3m)	30s	No	1	class: os component: system scope: availability •••

Time ▾	☐	Severity	Recovery time	Status	Info	Host	Problem	Duration	Ack	Actions	Tags
10:24:09	☐	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?

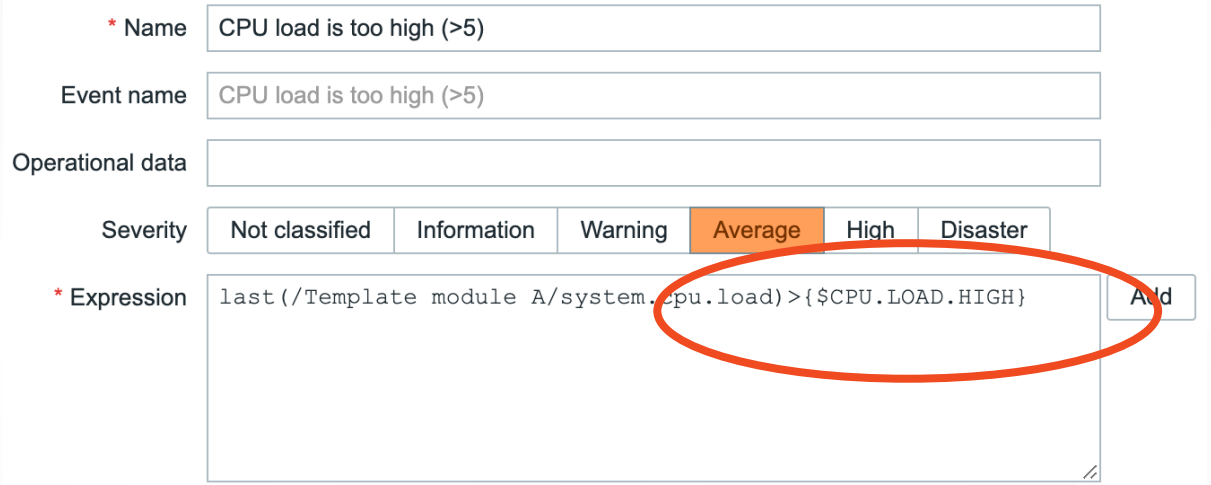
Thresholds

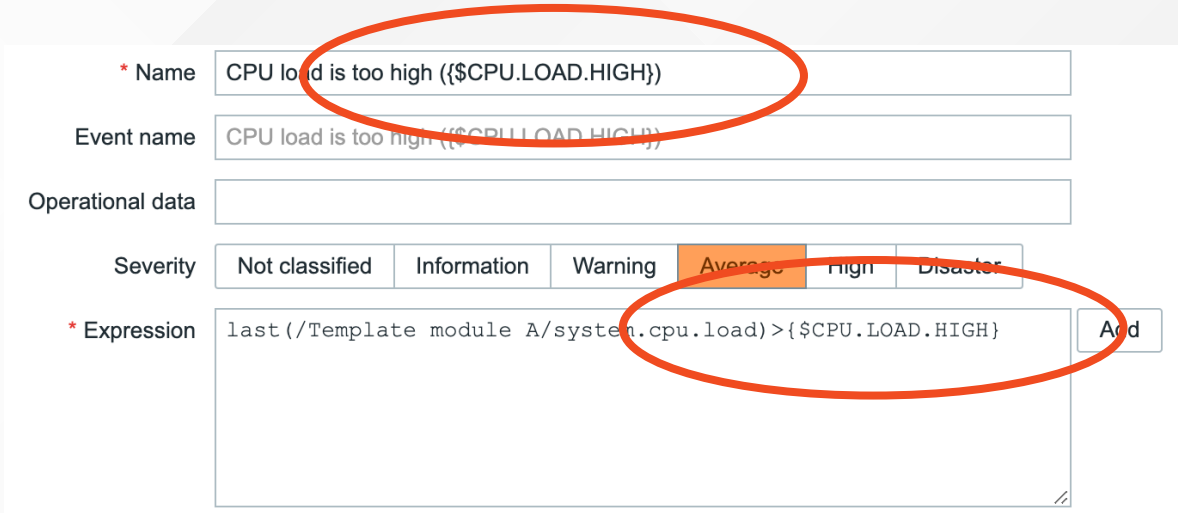
- If the last value that came is, is above 5, go into problem state



Macros

- Change static threshold to macros!





Operational data

- Monitoring –> Problems

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

Displaying 1 of 1 found

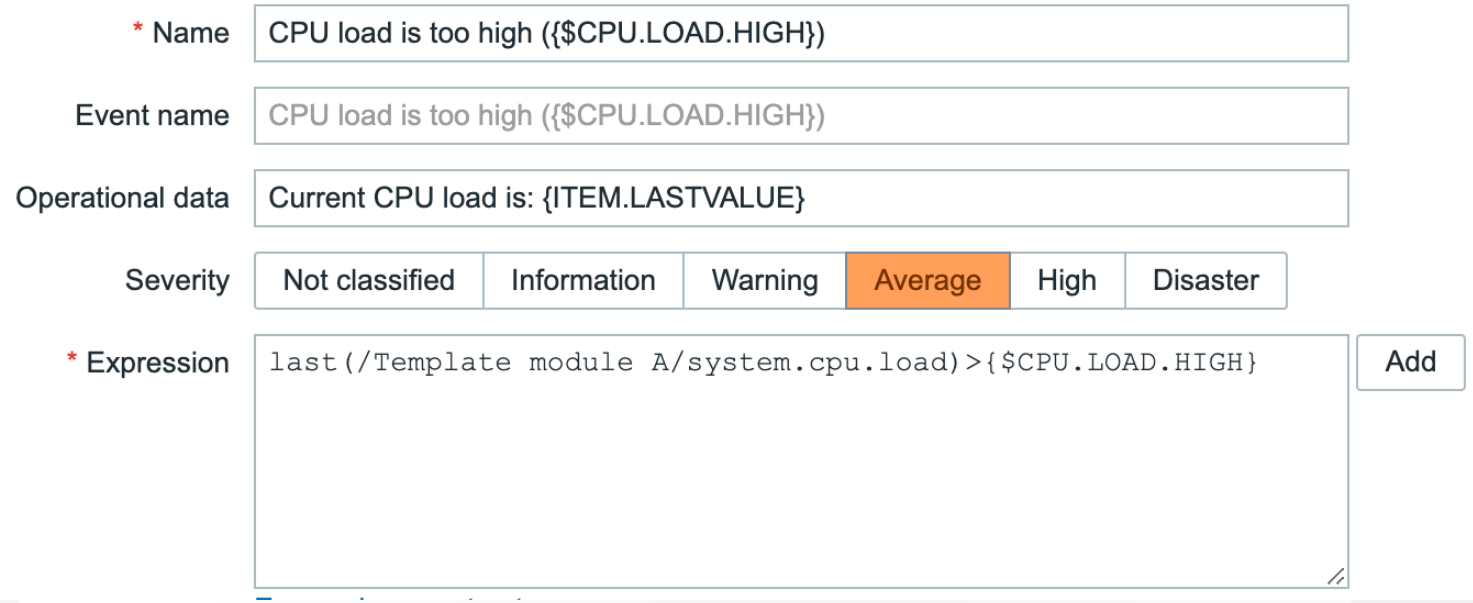
Show operational data: None | Separately | With problem name

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

Displaying 1 of 1 found

Operational data

- Trigger configuration



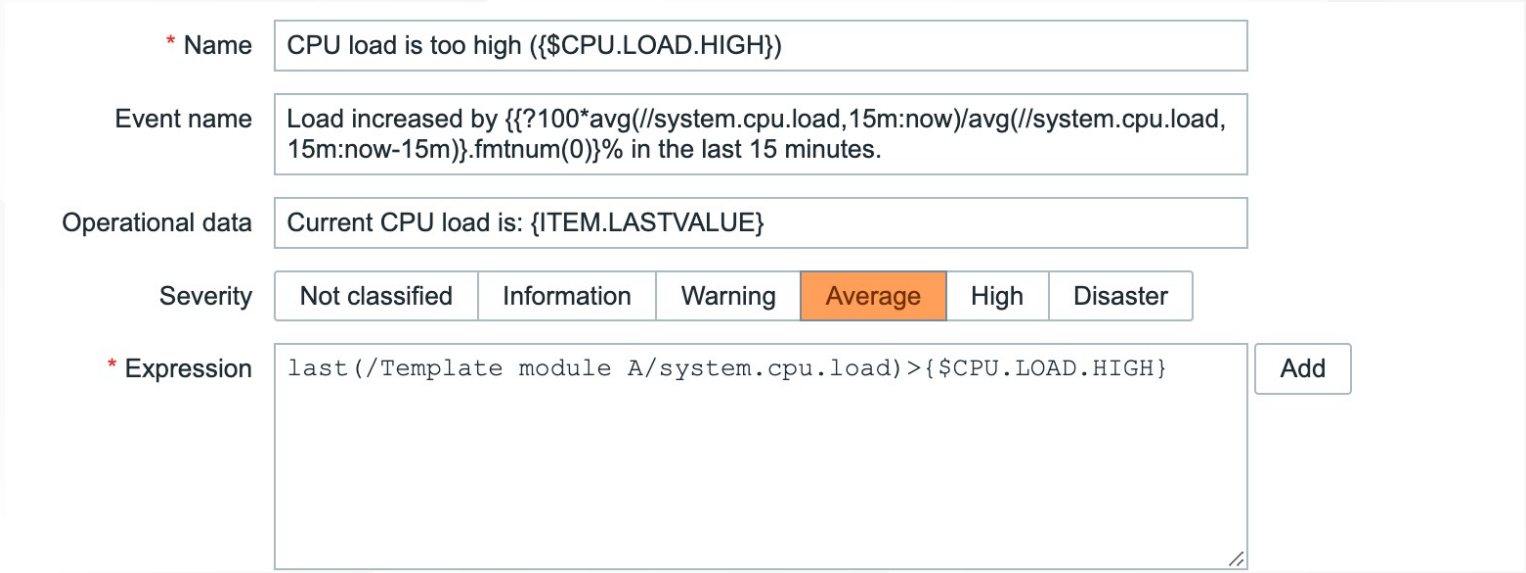
- Problem name

Time	Severity	Recovery time	Status	Info	Host	Problem	Operational data	Duration	Ack	Actions	Tags
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

Event name

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

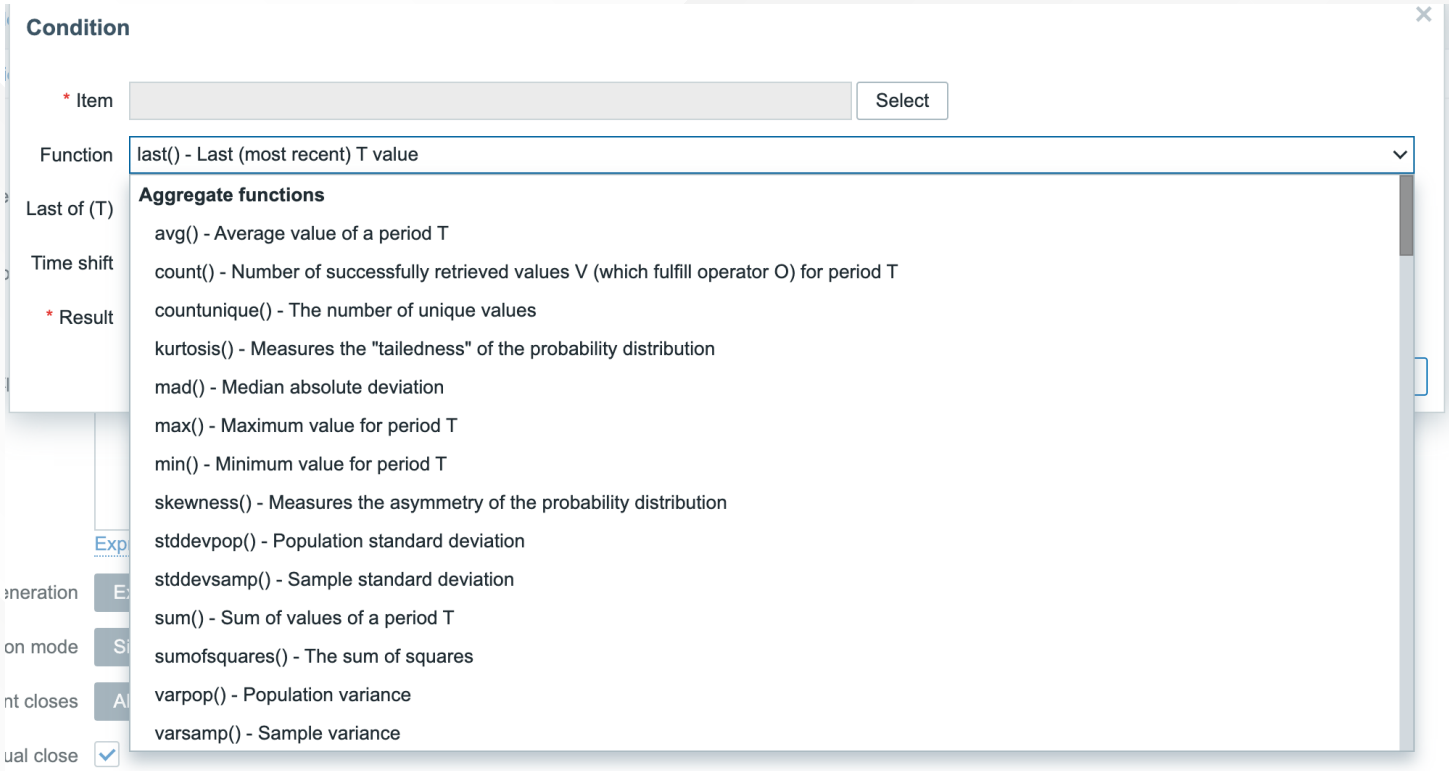


Time	Severity	Info	Host	Problem	Operational data	Duration	Ack	Actions	Tags
19:29:32	Average		host	Load increased by 174% in the last 15 minutes.	Current CPU load is: 2.11	1s	No		

Displaying 1 of 1 found

Functions

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



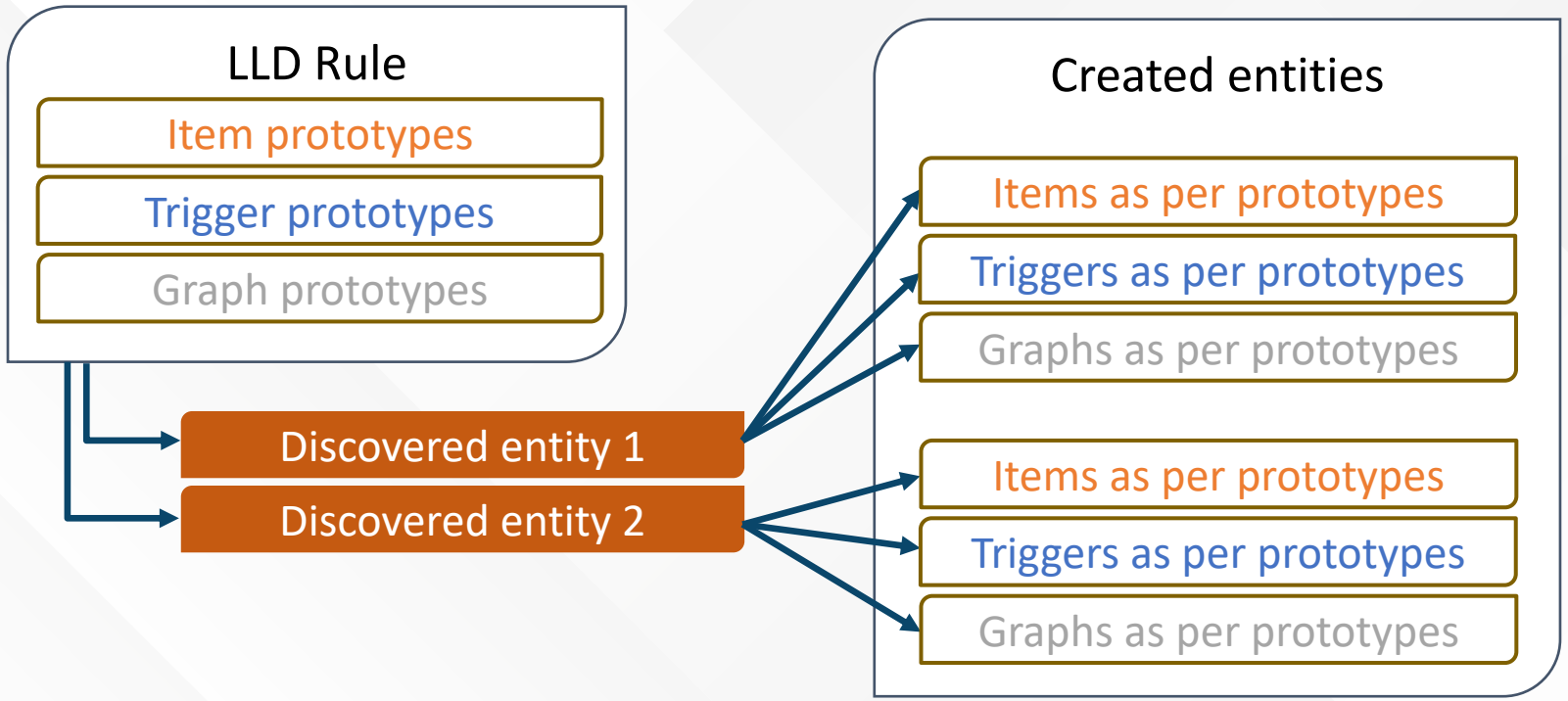
Low Level Discovery

- 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

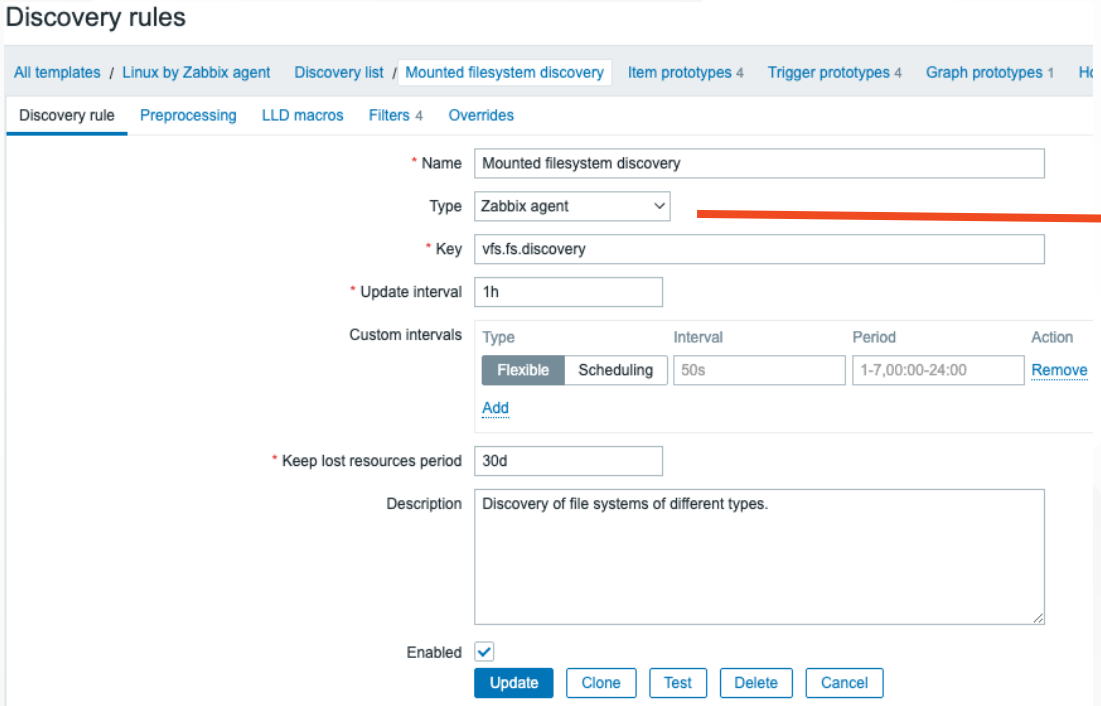
Workflow

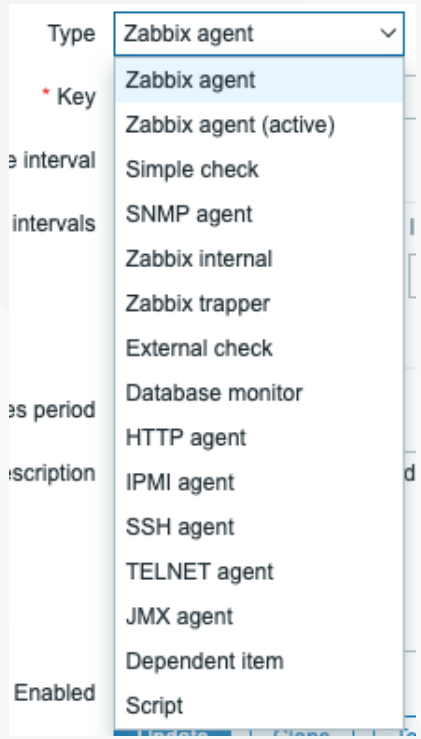
- Create discovery rule
- Define prototypes (of items, triggers etc)



Discovery rule

- Can be created on template or host level



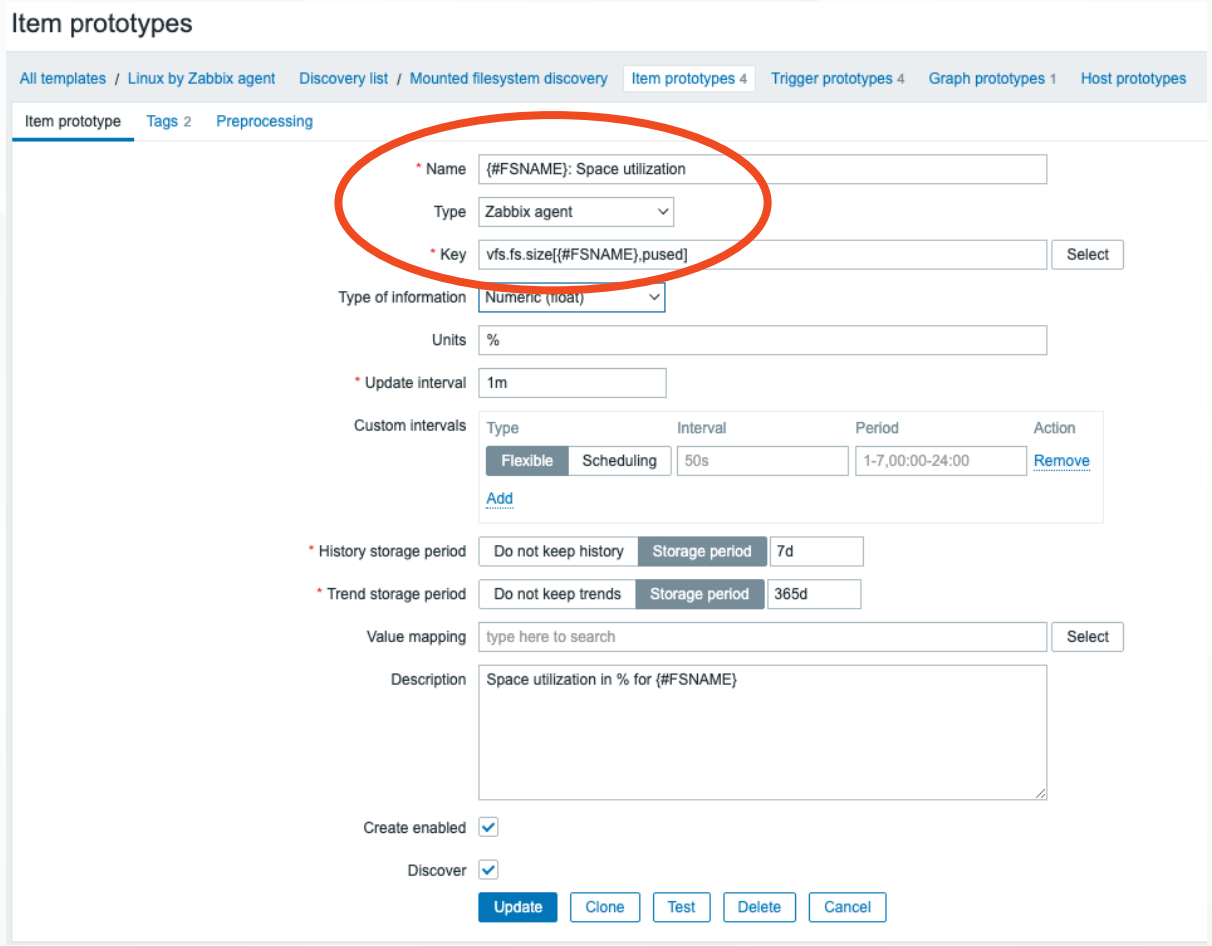


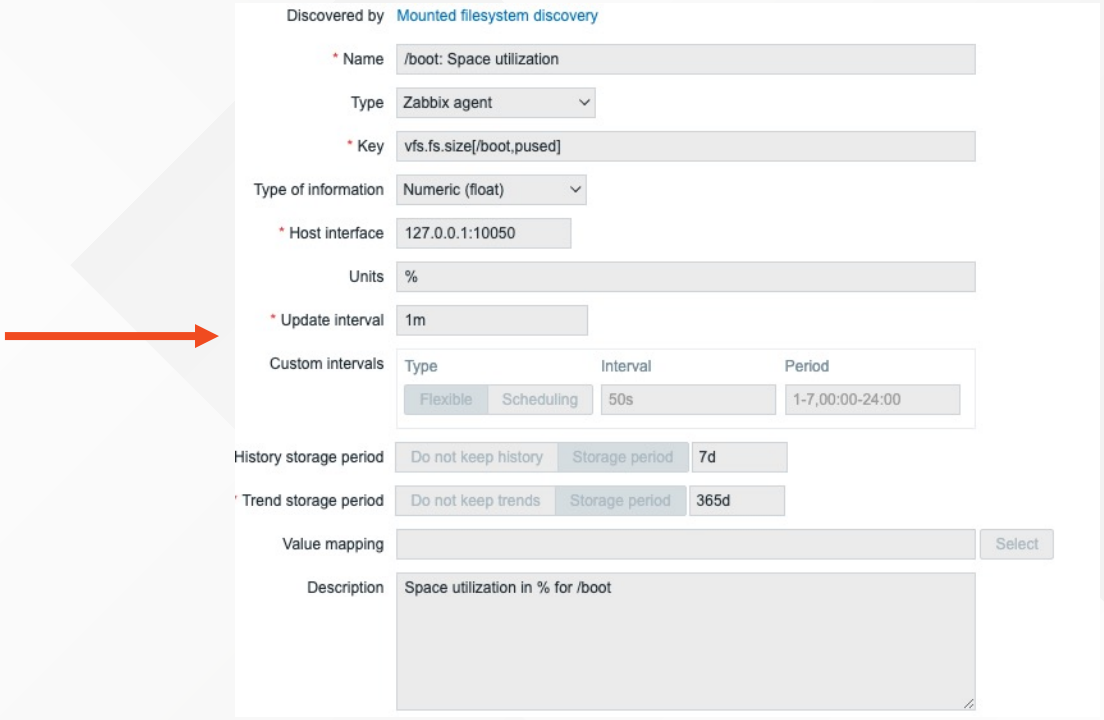
Discovery rule 2

- 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





Trigger prototype

* Name	{#FSNAME}: Disk space is low
Event name	{#FSNAME}: Disk space is low (used > {$VFS.FS.PUSED.MAX.WARN:"{#FSNAME}"}%)
Operational data	Space used: {ITEM.LASTVALUE3} of {ITEM.LASTVALUE2} ({ITEM.LASTVALUE1}
Severity	Not classified | Information | **Warning** | Average | High | Disaster
* Expression	Add

```
last(/Linux by Zabbix agent/vfs.fs.size[{#FSNAME},pused])>{$VFS.FS.PUSED.MAX.WARN:"{#FSNAME}"}
and
(
  (
    last(/Linux by Zabbix agent/vfs.fs.size[{#FSNAME},total])
    -
    last(/Linux by Zabbix agent/vfs.fs.size[{#FSNAME},used])
  ) <{$VFS.FS.FREE.MIN.WARN:"{#FSNAME}"}
or
  timeleft(/Linux by Zabbix agent/vfs.fs.size[{#FSNAME},pused],1h,100)<1d
)
```

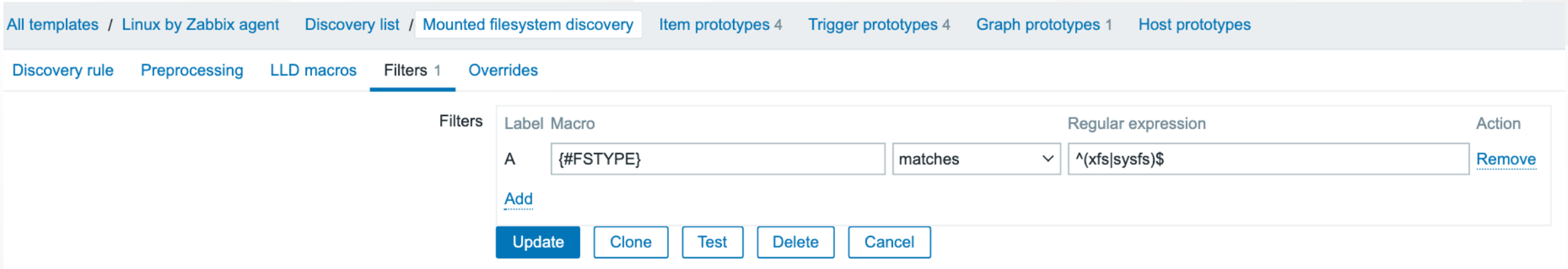
Expression constructor

Time	Severity	Info	Host	Problem	Duration	Ack	Actions	Tags
12:17:36	Warning		Zabbix server	/boot: Disk space is low (used > 5%)	1m 9s	No		class: os component: storage filesystem: /boot

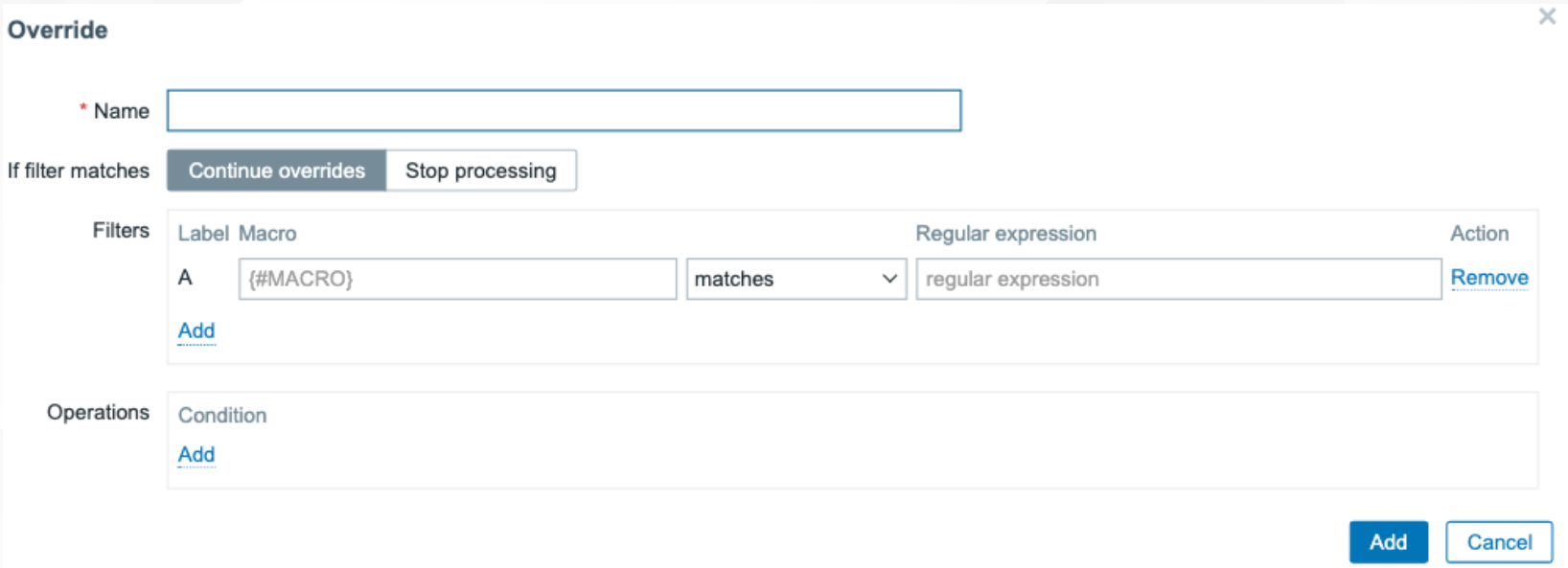
Filters

- By default, ALL discovered entities will be added
- This might be NOT what you want, because a lot of ‘useless’ information might come in

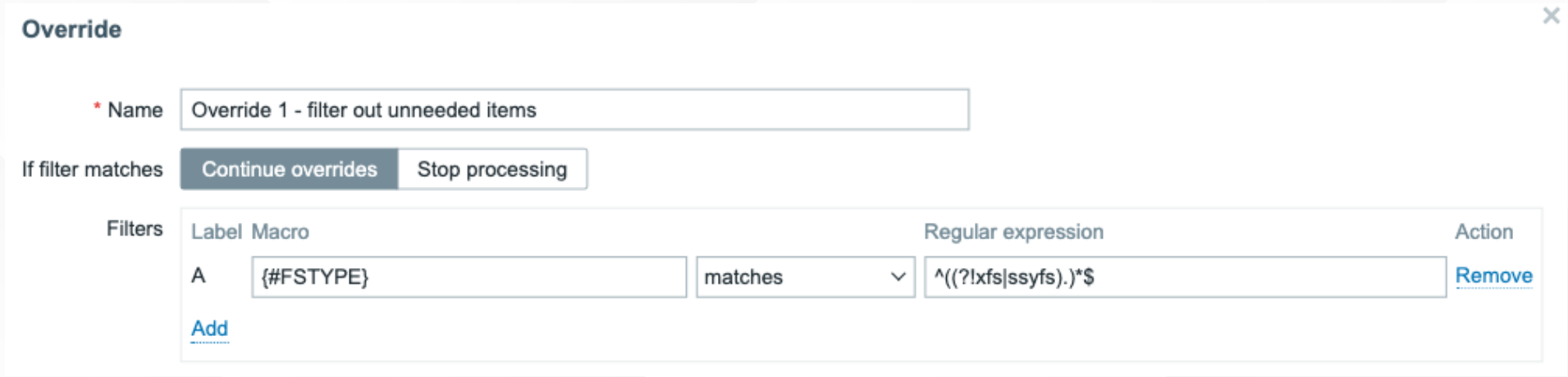
- Filters are **one** way of fixing this:

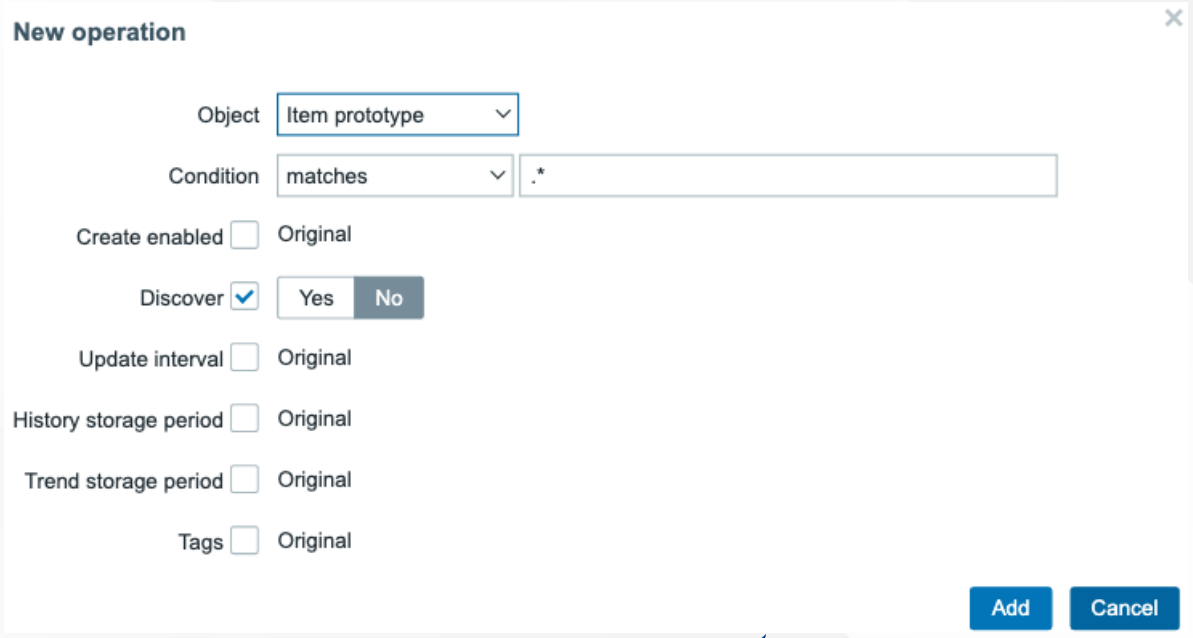


Override - filter



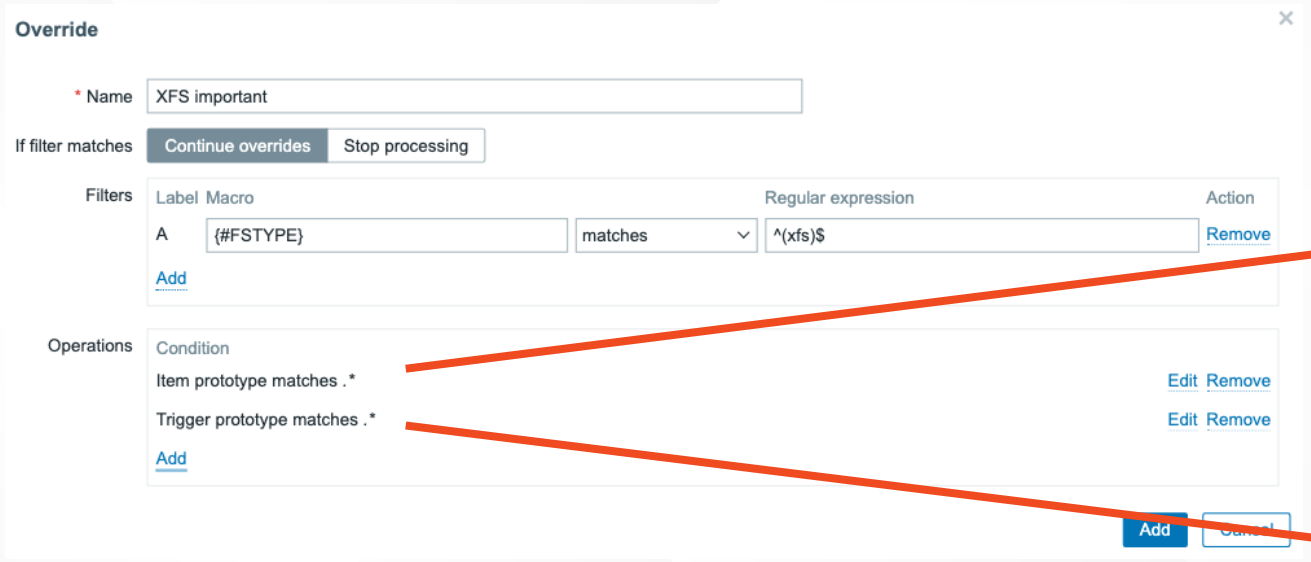
Override - filter

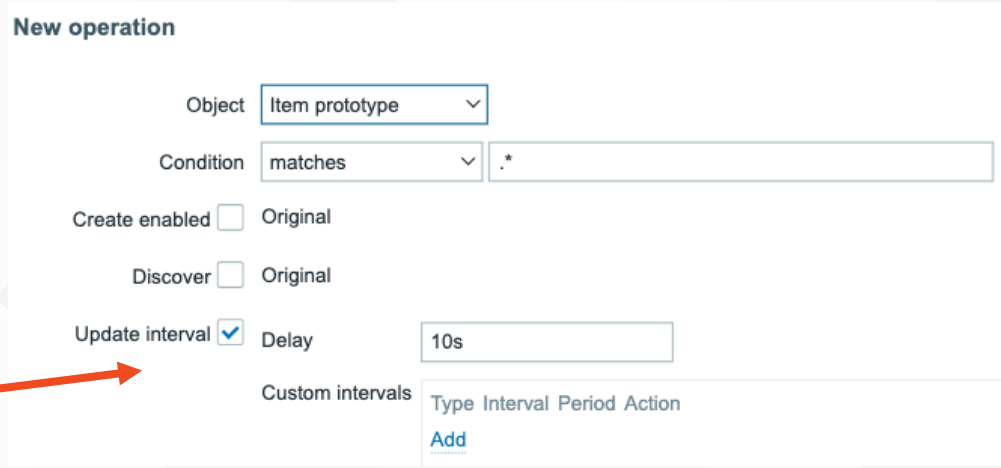


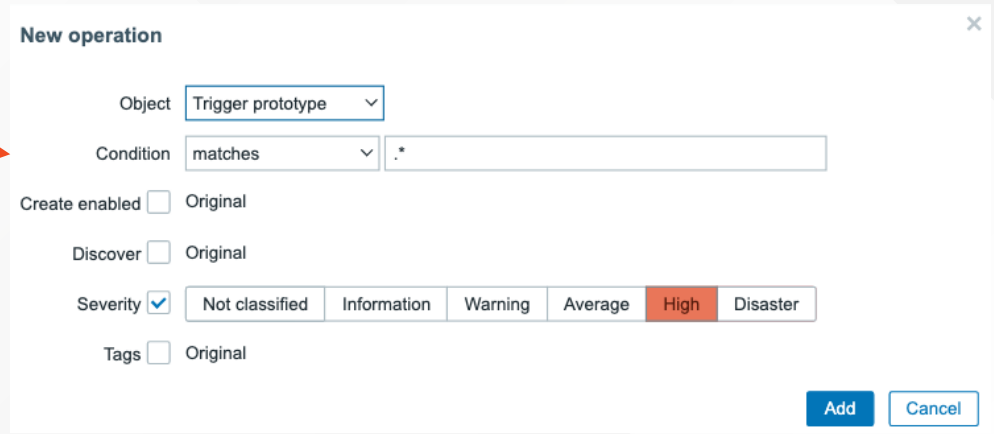


Override per item match

- Overrides are extremely flexible







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

Closing

- 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