ZABBIX 5.0

Certified Specialist Training

Day 4

COPYRIGHT NOTICE

Rules

It is prohibited to make any video and/or audio recordings during the whole period of this course.

This course is intended only for the officially enrolled student. Subject to the Copyright Notice below, the student is not allowed to share his credentials for attending this course, to allow others to join and take part, or otherwise make use of these Materials.

Copyright notice

AGENDA

Reports

Inventory

Notifications
&
Escalations

Detection
of
Misconfiguration

Maintenance

Business Level
Monitoring (SLA)

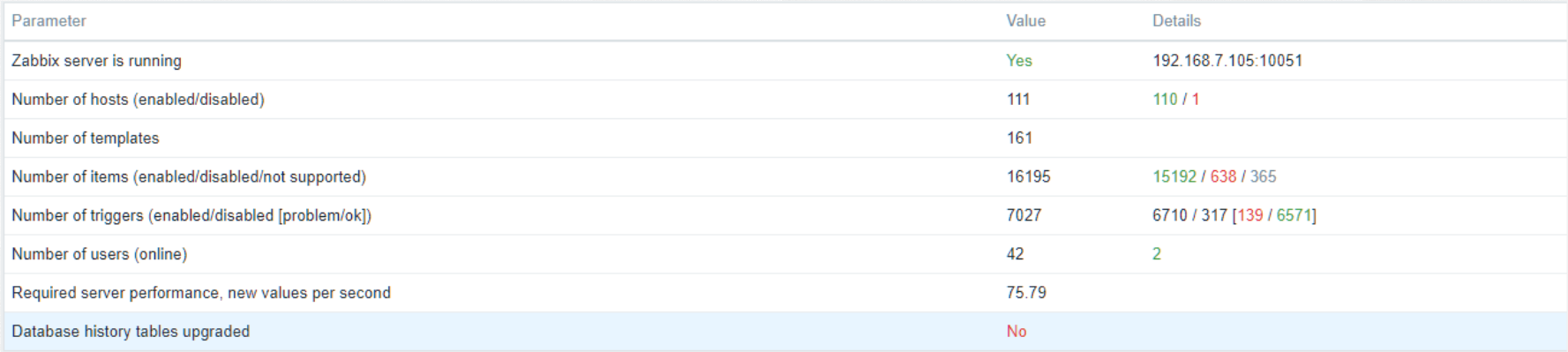
Low Level Discovery
&
Automation

XML
import/export

Backups

Reports

Reports > System information



Parameter	Value	Details
Zabbix server is running	Yes	192.168.7.105:10051
Number of hosts (enabled/disabled)	111	110 / 1
Number of templates	161	
Number of items (enabled/disabled/not supported)	16195	15192 / 638 / 365
Number of triggers (enabled/disabled [problem/ok])	7027	6710 / 317 [139 / 6571]
Number of users (online)	42	2
Required server performance, new values per second	75.79	
Database history tables upgraded	No	

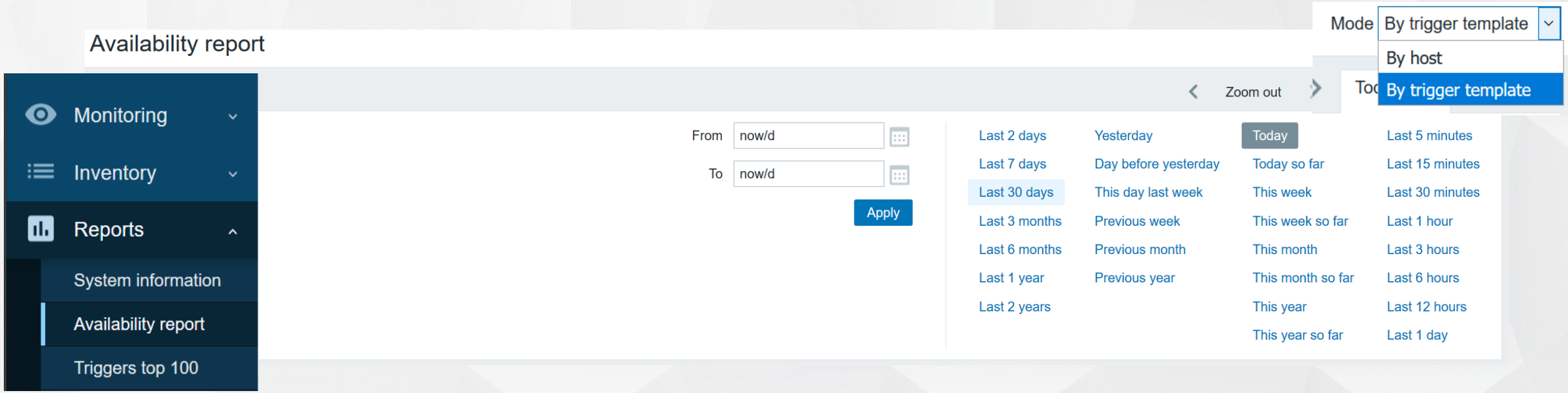
Parameter	Value	Details
Zabbix server is running	Whether Zabbix server is running: **Yes/No**	Location and port of Zabbix server
Number of hosts	Total number of hosts	Number of monitored/not monitored hosts
Number of templates	Total number of templates	
Number of items	Total number of items	Number of monitored/disabled/unsupported items
Number of triggers	Total number of triggers	Number of enabled/disabled triggers. [Triggers in problem/ok state.]
Number of users	Total number of users configured	Number of users online
Required server performance new values per second	The expected number of new values per second	Required server performance is an estimate and can be useful as a guideline
Database history tables upgraded	Whether history table is using double float datatype: **Yes/No**	History table must be manually upgraded if migrated from previous version

For precise numbers of values processed, use the zabbix[wcache,values,all] internal item

https://www.zabbix.com/.../frontend_sections/reports/status_of_zabbix_

AVAILABILITY REPORT

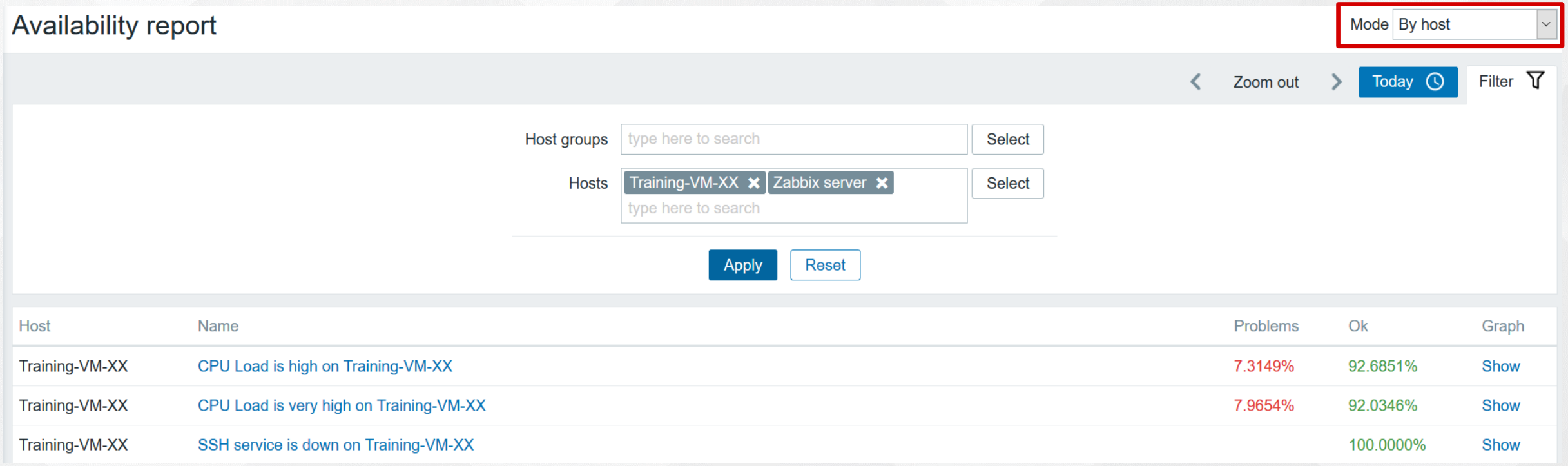
- Proportion of time each trigger has been in the problem/ok state:
  - is displayed as percentage
  - easy to determine the availability
- You can choose the mode:
  - triggers by host
  - by triggers belonging to a template
- The time period selector allows to select often required periods with one mouse click.



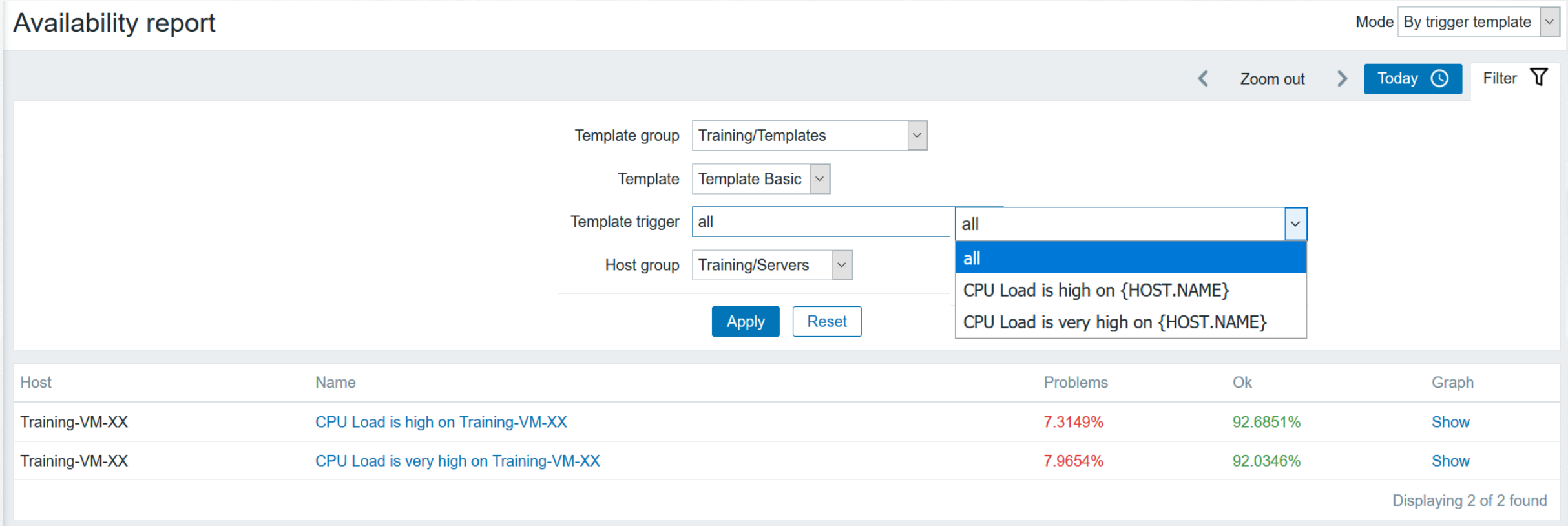
.../5.0/manual/web_interface/frontend_sections/reports/availability

Triggers by hosts availability report:

- set the time frame
- filter by host groups or hosts



Triggers belonging to a template:

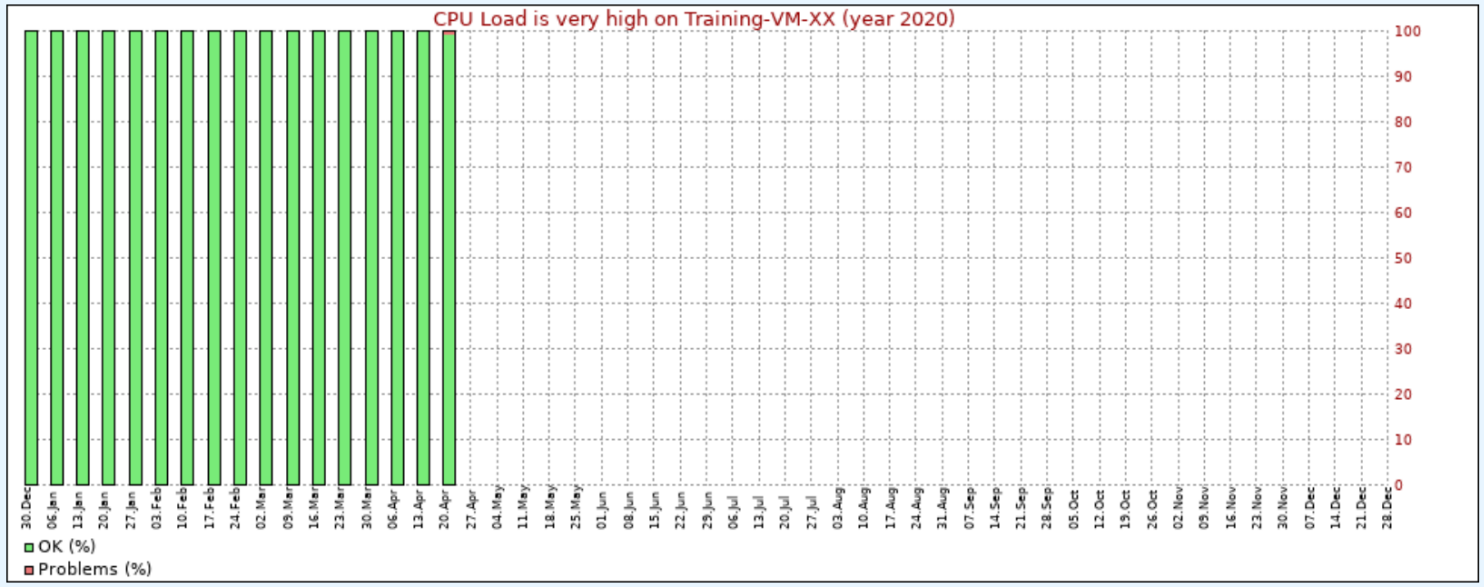


Clicking on Show in the Graph column opens a bar graph:

Problems	Ok	Graph
7.3149%	92.6851%	Show
7.9654%	92.0346%	Show
	100.0000%	Show

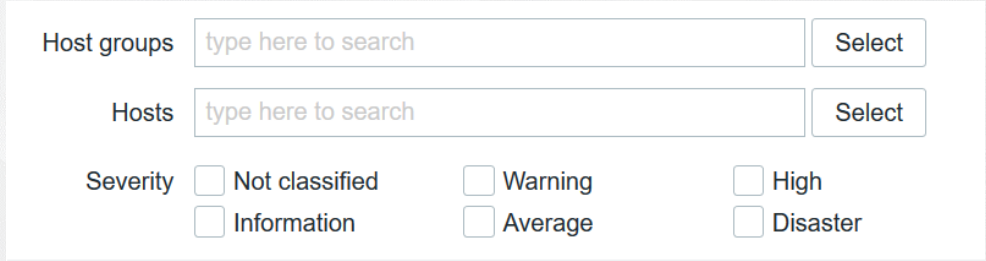
Availability report

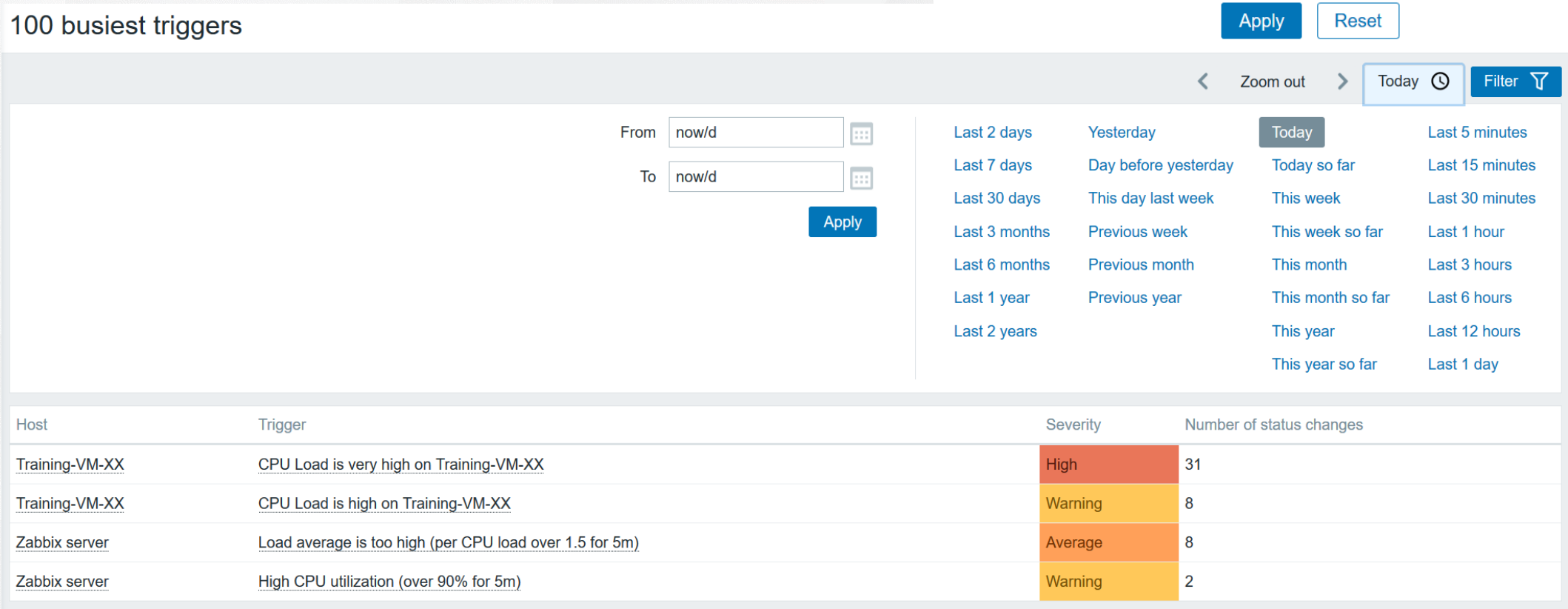
Training-VM-XX CPU Load is very high on Training-VM-XX



Triggers that have changed their state most often:

- Set the period of evaluation and adjust filters
- Sorted by the number of status changes
- Useful to detect flapping triggers





Host	Trigger	Severity	Number of status changes
Training-VM-XX	CPU Load is very high on Training-VM-XX	High	31
Training-VM-XX	CPU Load is high on Training-VM-XX	Warning	8
Zabbix server	Load average is too high (per CPU load over 1.5 for 5m)	Average	8
Zabbix server	High CPU utilization (over 90% for 5m)	Warning	2

Reports demo

Inventory Auto-collection

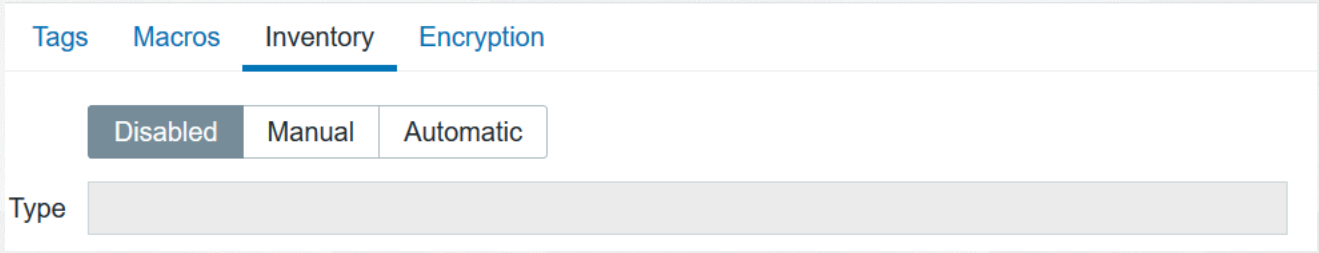
You can keep the inventory of devices and applications in Zabbix

- In the inventory tab you can enter such details as name, serial number, location, etc.
  - Inventory fields are hardcoded
- Default inventory mode for new hosts is defined in Administration > General > Other
  - By default, it is set to "disabled"
  - Inventory mode for a host can be changed in the host configuration form
- Populating inventory can be done manually or automatically
  - Manual mode – you can enter the details including type, location, etc.
  - Automatic mode - items can be used to add data to inventory
- Autoregistration and Network discovery actions can override discovery mode for new or existing hosts

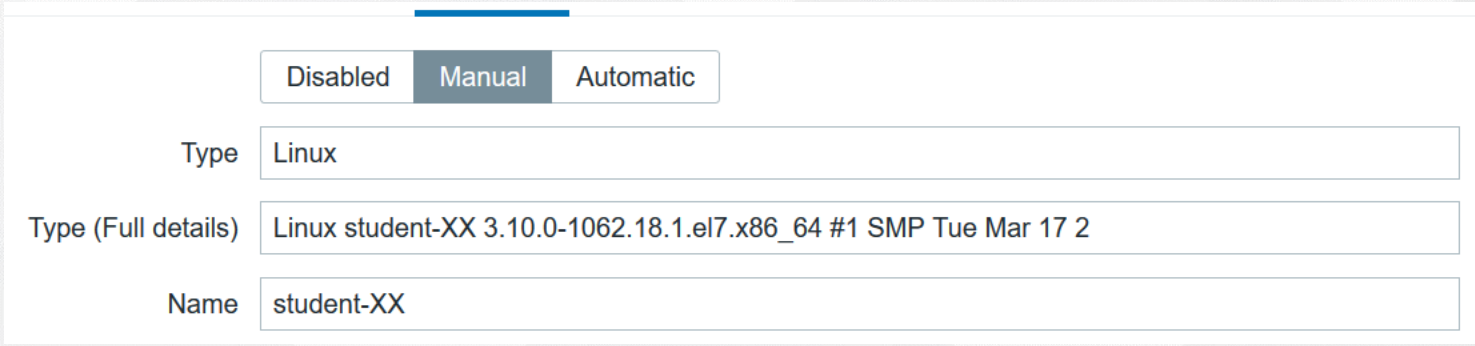
https://www.zabbix.com/documentation/5.0/manual/config/hosts/inventory

Configuration > Hosts > {Host} > Host inventory

- By default: inventory is disabled

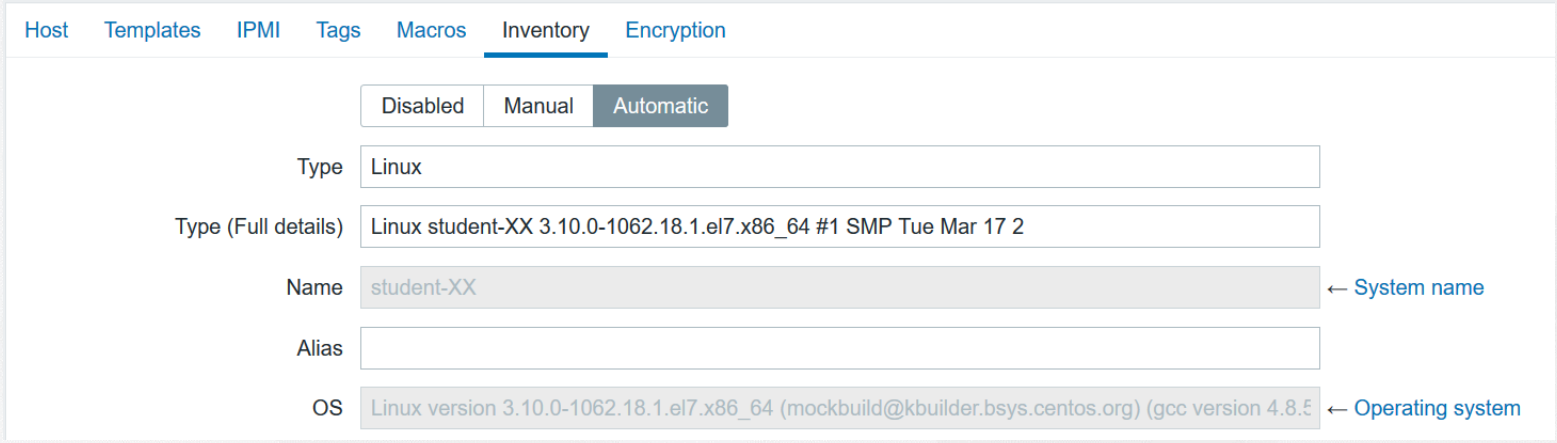


- Set to Manual and fill in necessary fields



1. Host inventory mode must be set to Automatic

- Configuration > Hosts > {host} > Inventory



2. Configure an item to populate inventory field with value

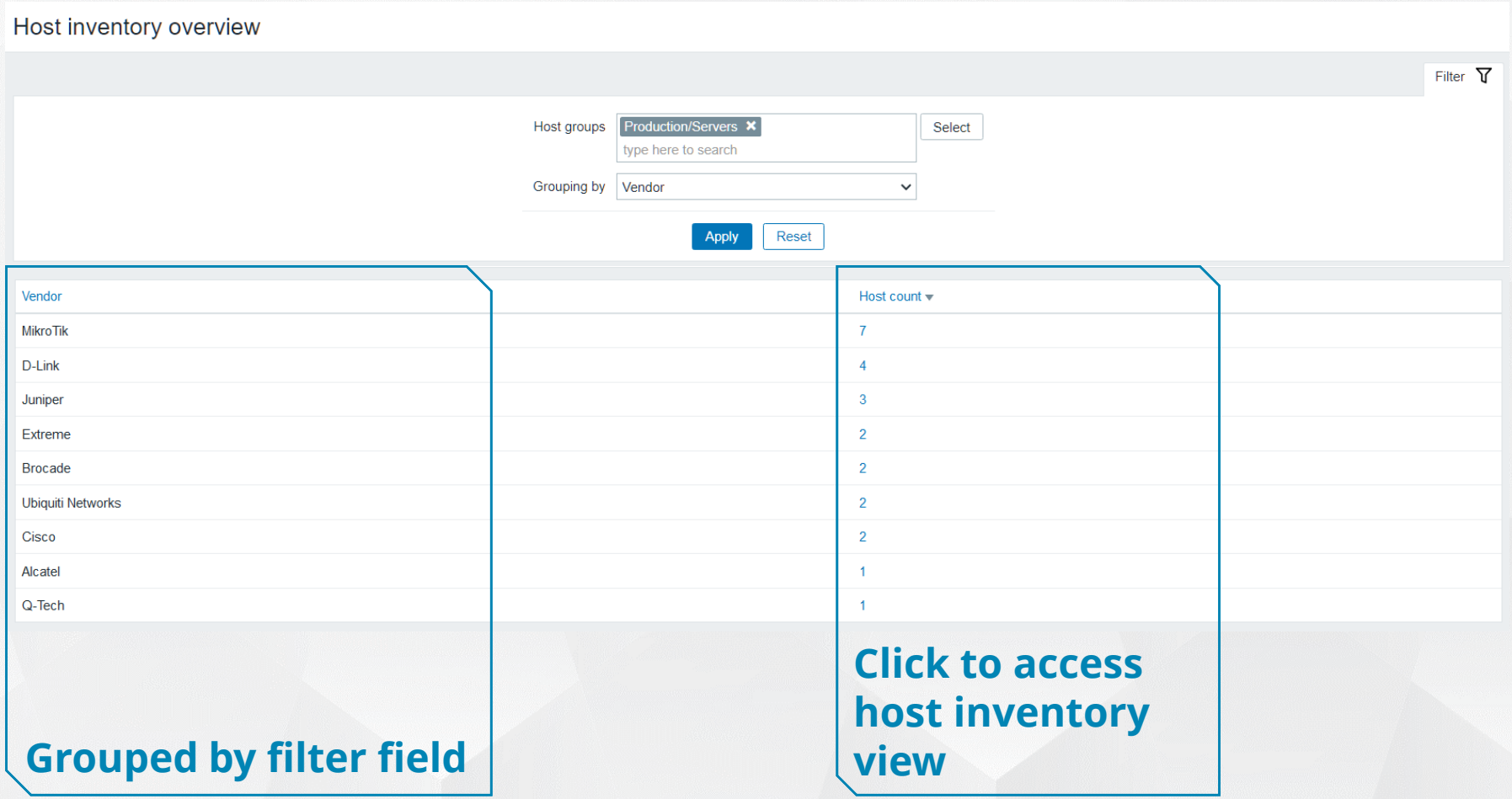
- Configuration > Hosts > {host} > Items > <Item>

Items that are especially useful for automated inventory data collection:

- system.uname - identification of the system
- system.hostname - system host name
- system.hw.chassis[full|type|vendor|model|serial] - default is [full], need root
- system.hw.devices[pci|usb] - default is [pci]
- system.hw.macaddr[interface,short|full] - default is [all,full], interface is regexp
- system.sw.os[name|short|full] - default is [name]
- system.sw.packages[package,manager,short|full] - default is [all,all,full], package is regexp
- SNMPv2-MIB::sysLocation - device location
- SNMPv2-MIB::sysContact - contact person
- etc.

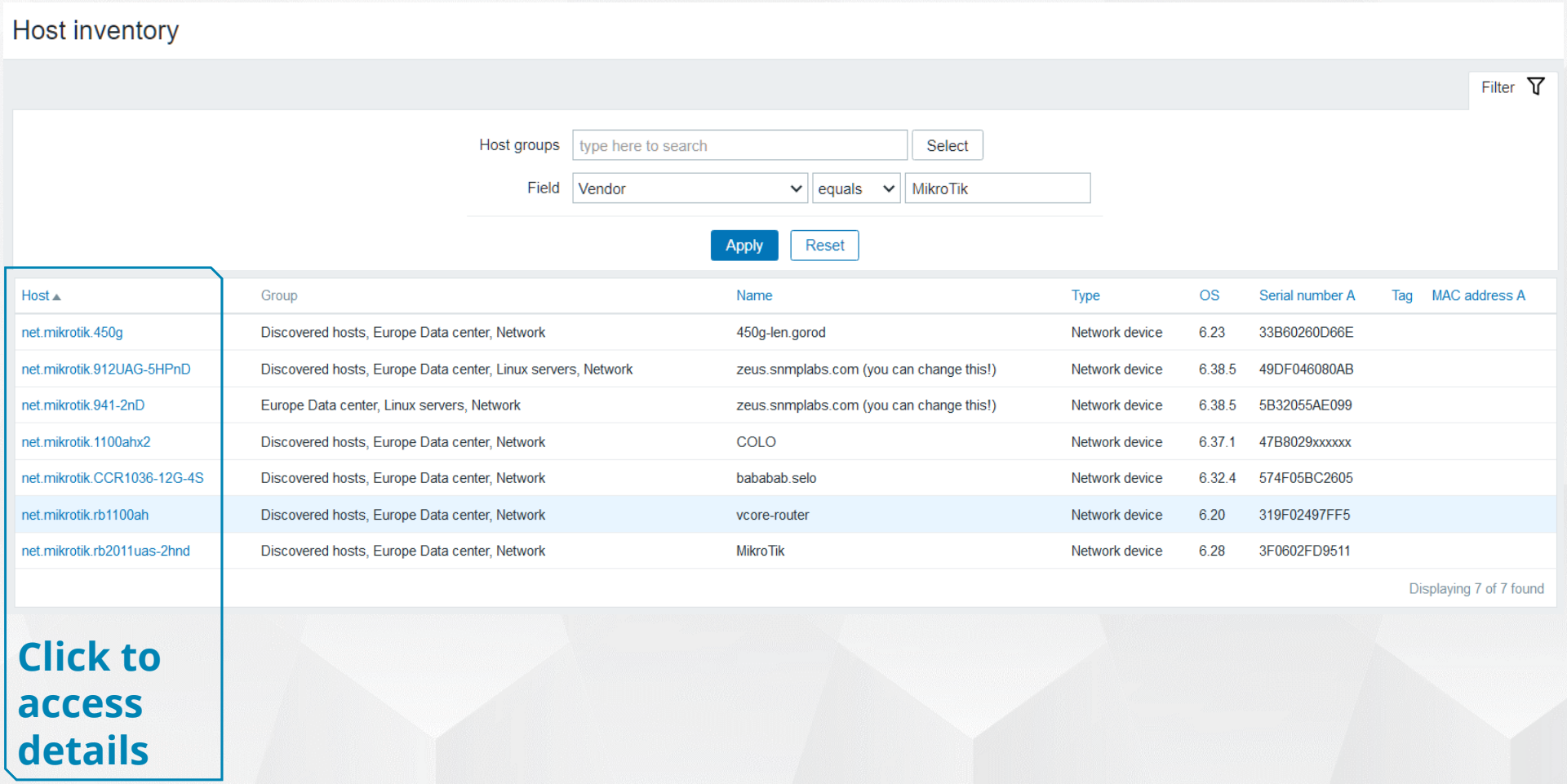
Inventory > Overview:

- Shows host count having the same inventory value
- Host count column entries are links to host inventory view



Inventory > Host inventory

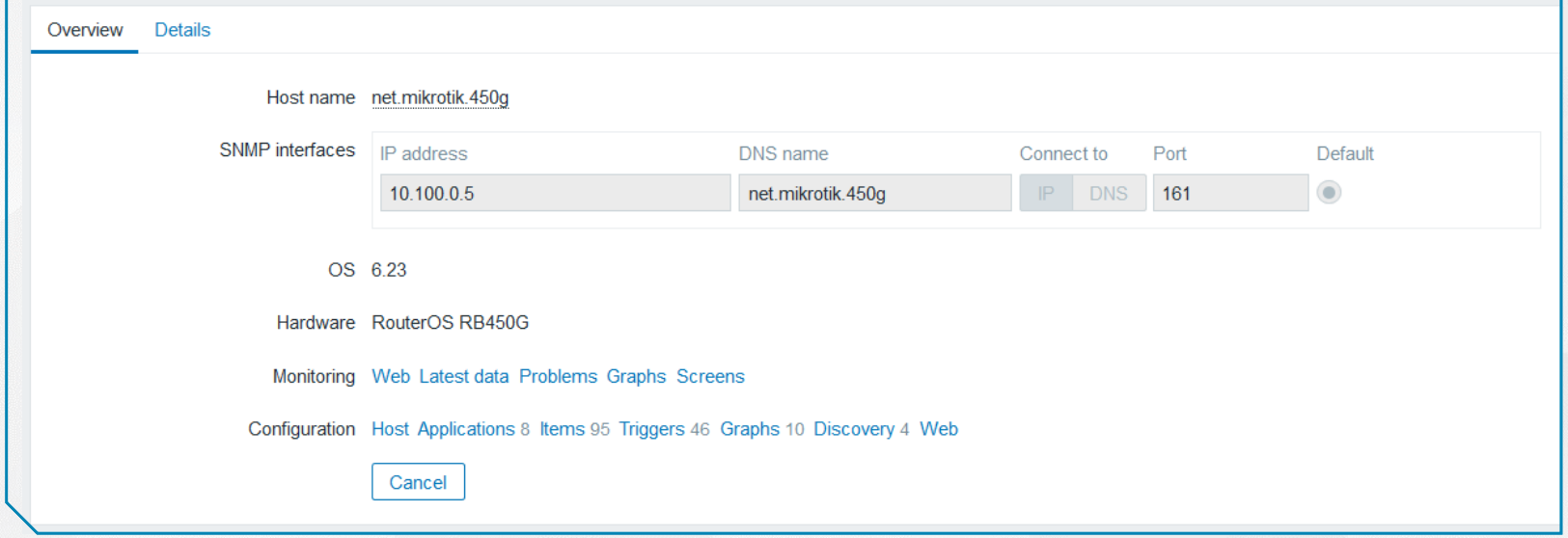
- Lists all hosts matching filter criteria
- Clicking on a host name will open the inventory details



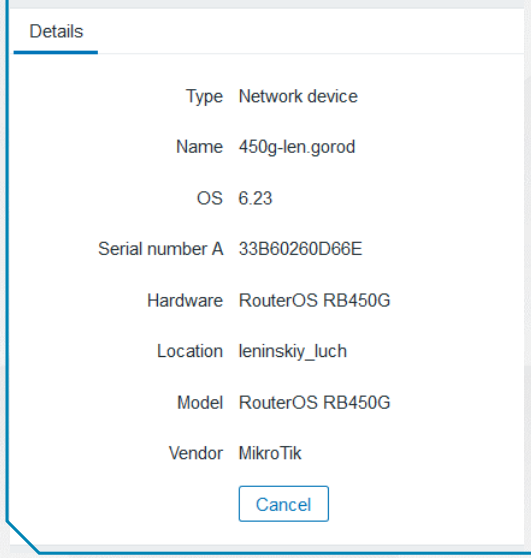
Inventory details:

- The form has two tabs:
  - General information page displays common information and has some usefull links
  - Details tab displays all inventory data collected from a host
- Can be accessed from Inventory view, Problems page and other frontend sections

general information about the host



all available inventory details



- Only one item can be used to populate an inventory field on same host
- Host inventory can be opened from different views (e.g. Dashboard, Maps, Problems, etc.)
- Inventory data can be used in the filters and actions
- There are host inventory macros {INVENTORY.*} available for use in notifications and tags
- There is no way to customize inventory fields - current list is hardcoded

PRACTICAL SETUP

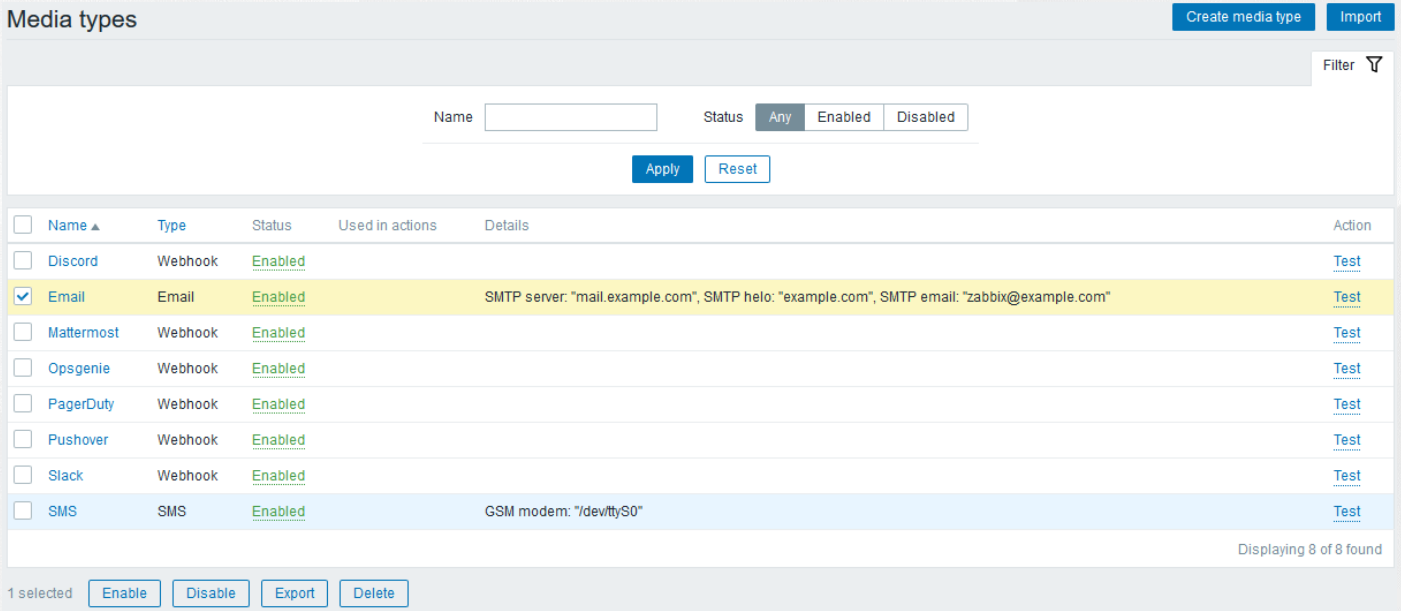
1. Enable automatic inventory mode for all hosts
2. Create a new template:
   - Name: Template Basic module system info
   - Group: Training/Templates
3. Create new Zabbix agent items
   1) System OS:
      - Use system.sw.os[name] key to get OS information
      - Populate inventory field: "OS”
   2) System hostname:
      - Find a key can to the hostname
      - Populate inventory field: Name
4. Link the template to ”Template Basic”
5. Manually populate inventory field Location for all hosts
6. Make sure that the tabs Overview and Details contain information

Notifications and Media types

Administration > Media types

Configure the ways for delivery of notifications and alerts

- Email
- SMS (Modem support)
- Webhooks
- Custom “ alert" scripts



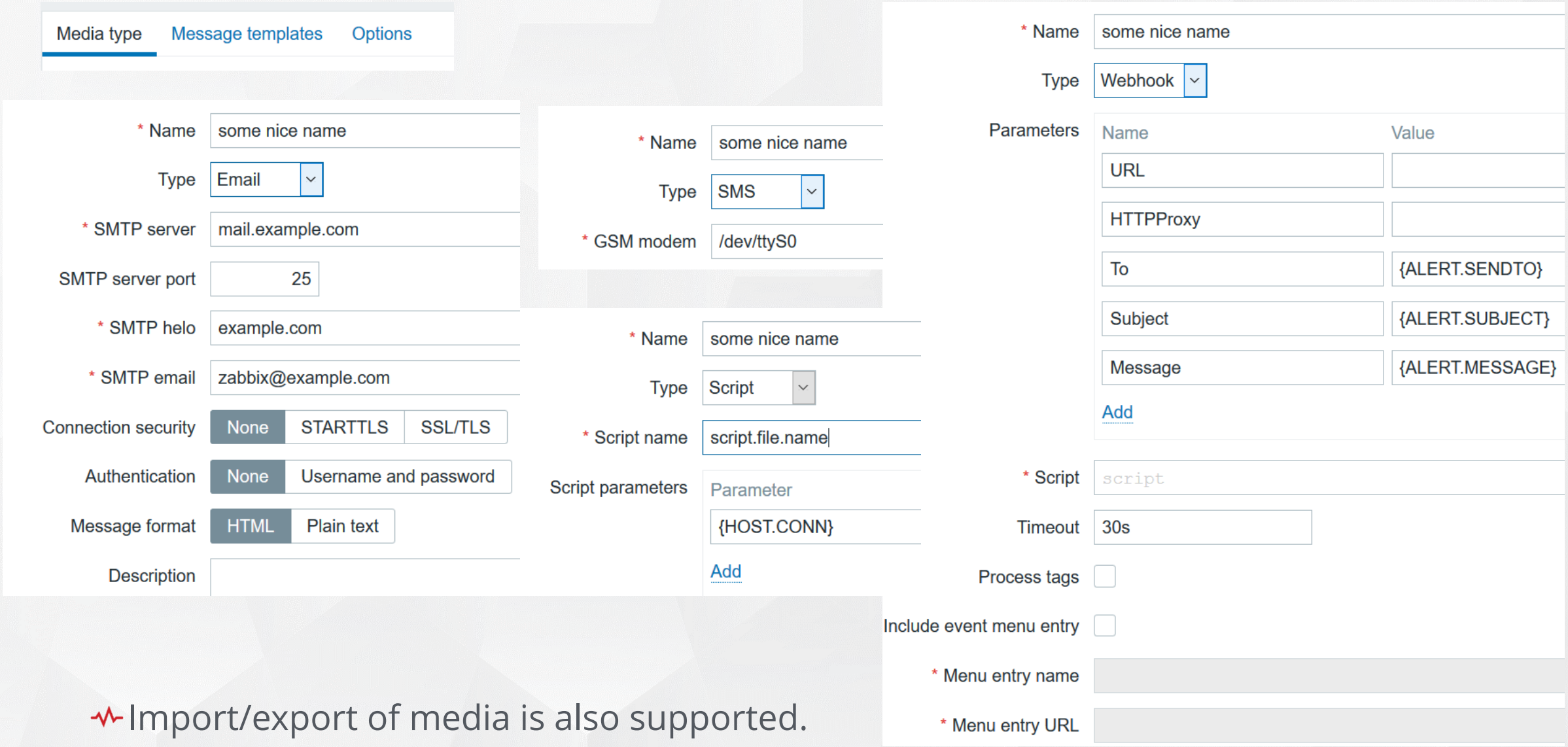
There are plenty of media types in the default dataset

- All you need is to finetune the parameters to make them work

Every media type can be tested directly from the frontend

Available only to Zabbix Super Administrators

To create a new media, press the [Create media type] button

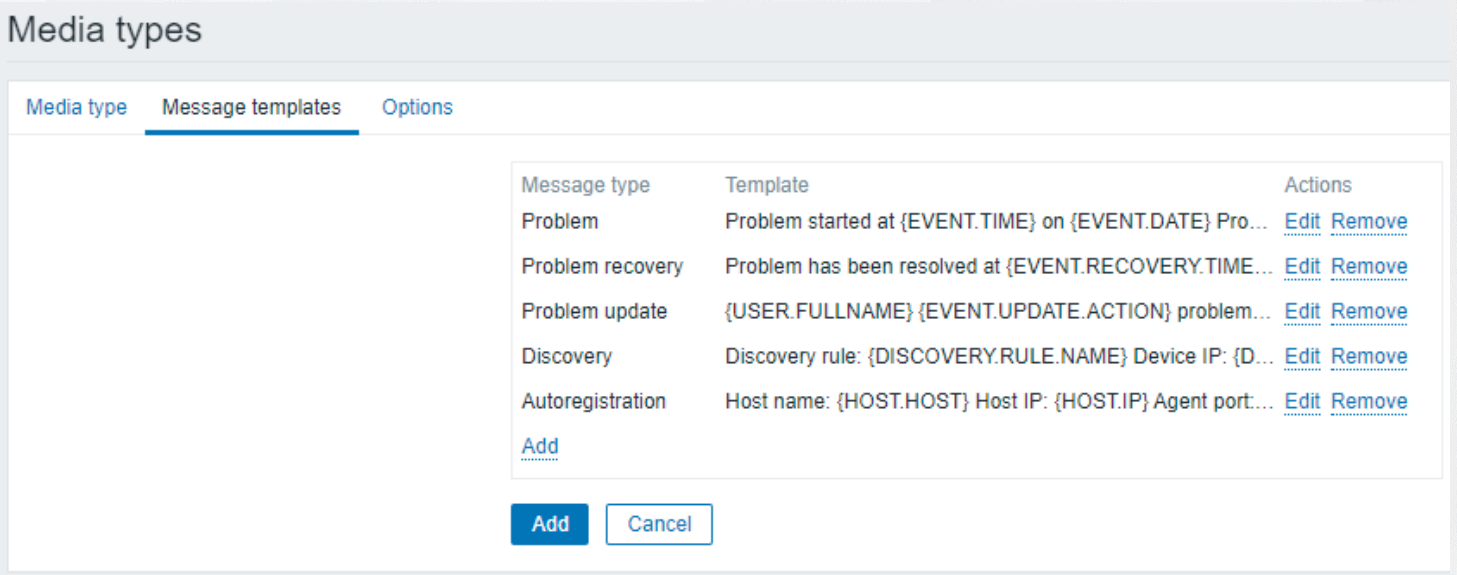


- Import/export of media is also supported.

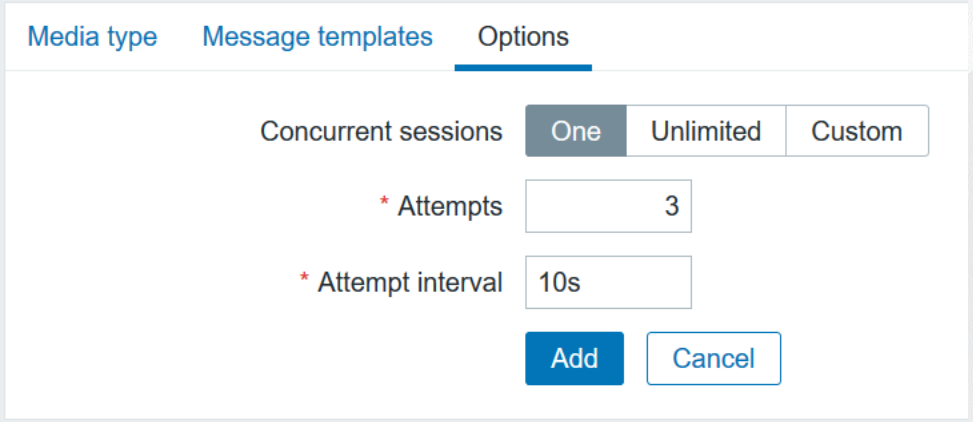
Administration > Media types > Message templates

Message type has 7 options:

- Problem
- Problem recovery
- Problem update
- Discovery
- Autoregistration
- Internal problem
- Internal problem recovery



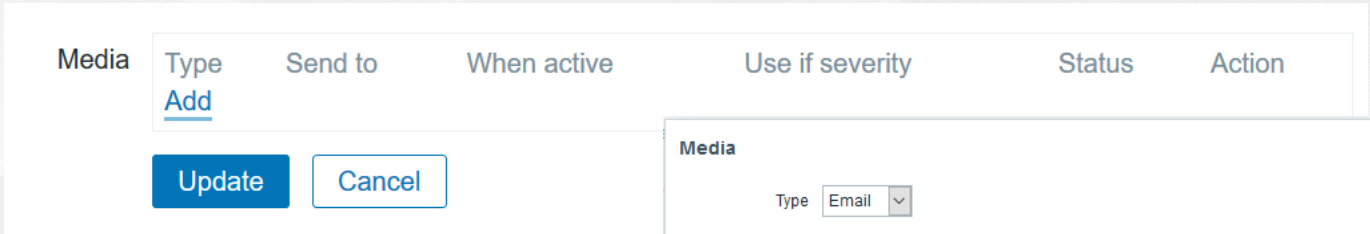
And additional options:

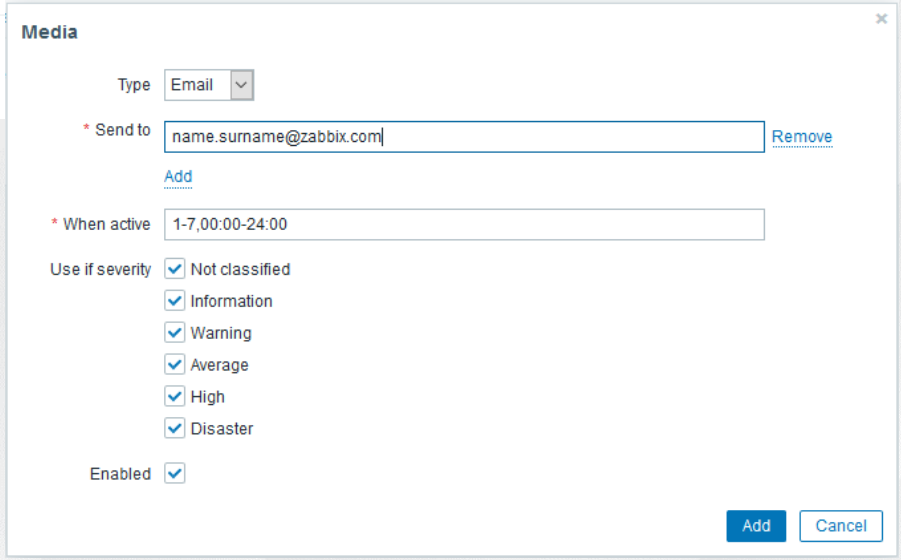


When creating a new media type - don't forget to create message templates for it!

In the user profile configuration form you can define your own media details

- Only Admin and Super Admin can change their own media details
- One or more user media
- Usually e-mail, phone number or other identifier
- Active based on:
  - Time period
  - Trigger severity



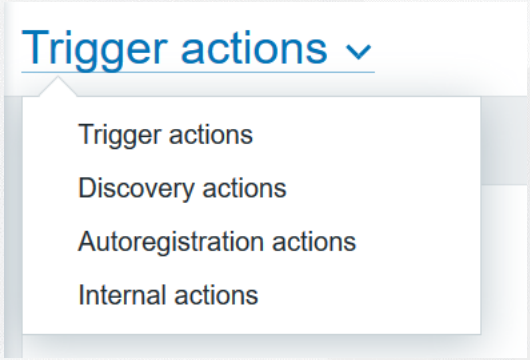


Actions and Escalations

Configuration > Actions

- A flexible set of conditions followed by automatically executed set of operations (notifications, remote commands, script execution etc.)

- Actions can be defined for:
  - Trigger events
  - Discovery events
  - Auto registration events
  - Internal events



https://www.zabbix.com/documentation/5.0/manual/config/notifications/action

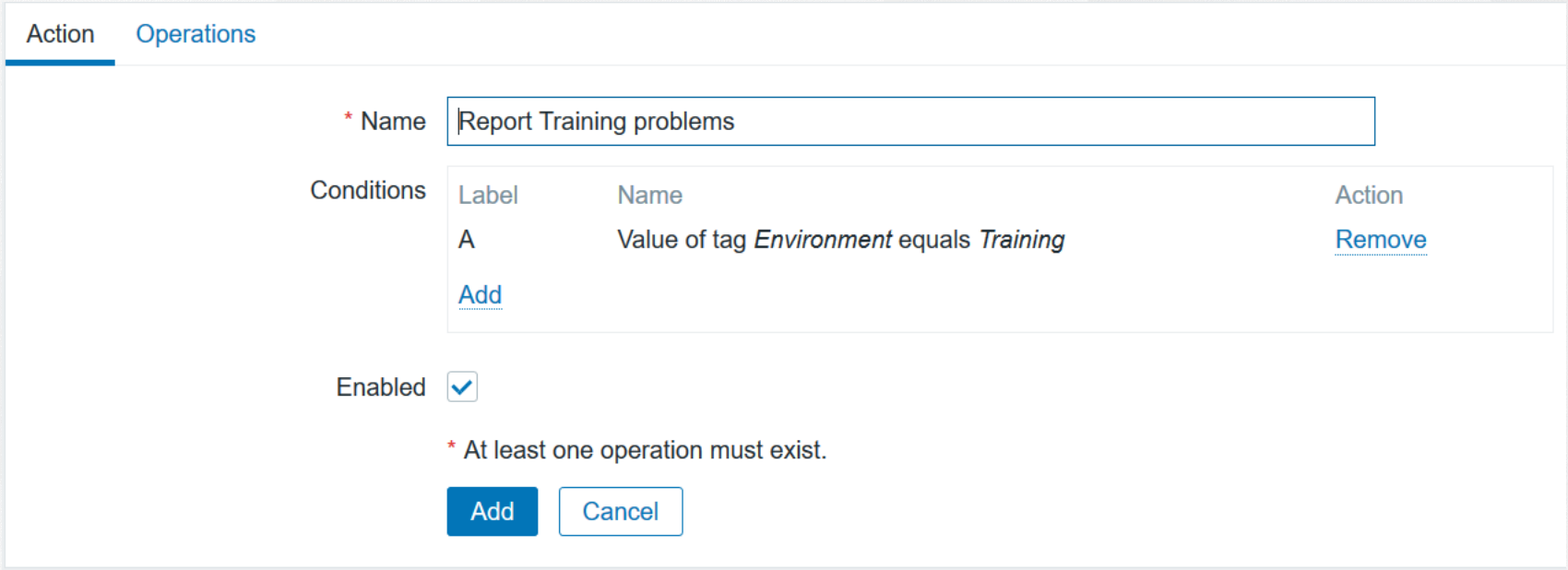
ACTIONS - FUNCTIONALITY

- Notify users
- Delayed notifications and remote commands
- Repeated notifications until the problem is resolved
- Different messages for acknowledged and unacknowledged problems
- Escalations to other users or user groups
- Unlimited number of escalation steps
- Execute remote commands :
  - On Zabbix server, proxy and agent
  - Via SSH and Telnet
  - Via IPMI
- Run global scripts and custom scripts
- Provide information with macros

Configuration > Actions > Trigger Actions > [Create action]

Available options:

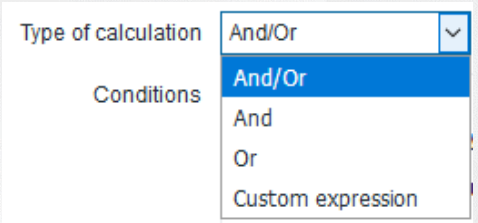
- Name
- Conditions
- Operations (Main, recovery and update)

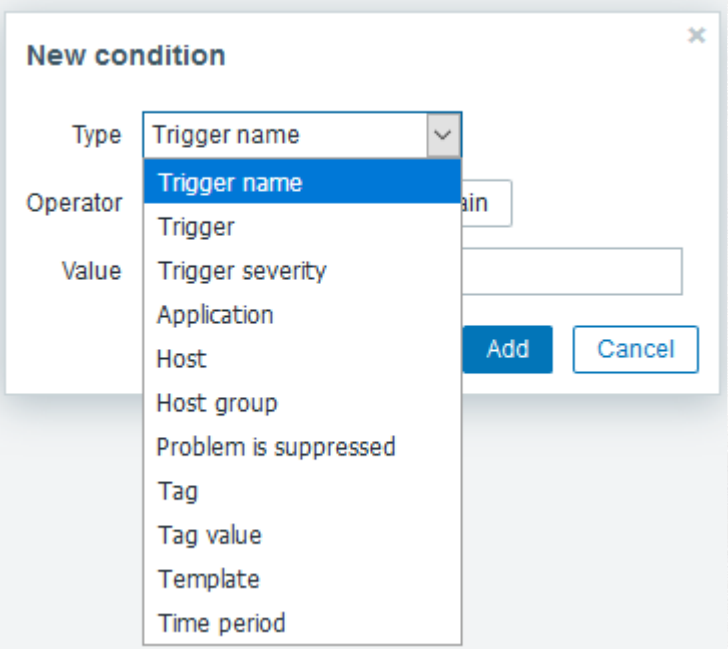


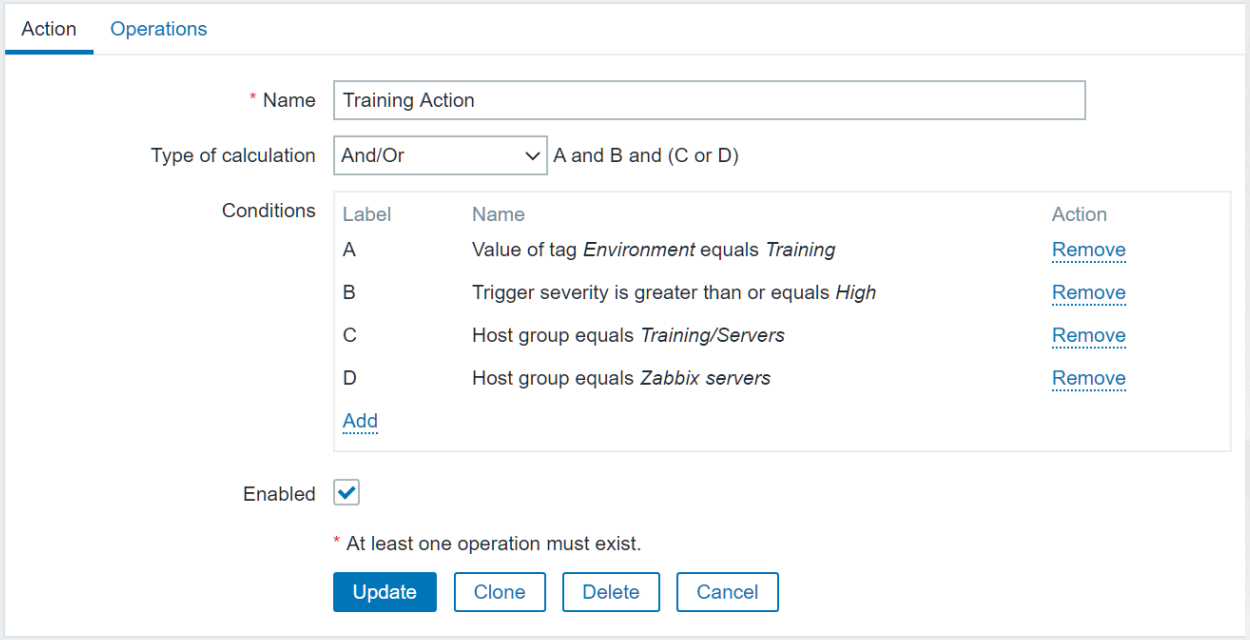
Flexible conditions:

- Host, host group
- Trigger name, severity or value
- Tag, Application, time period and more

Type of calculation



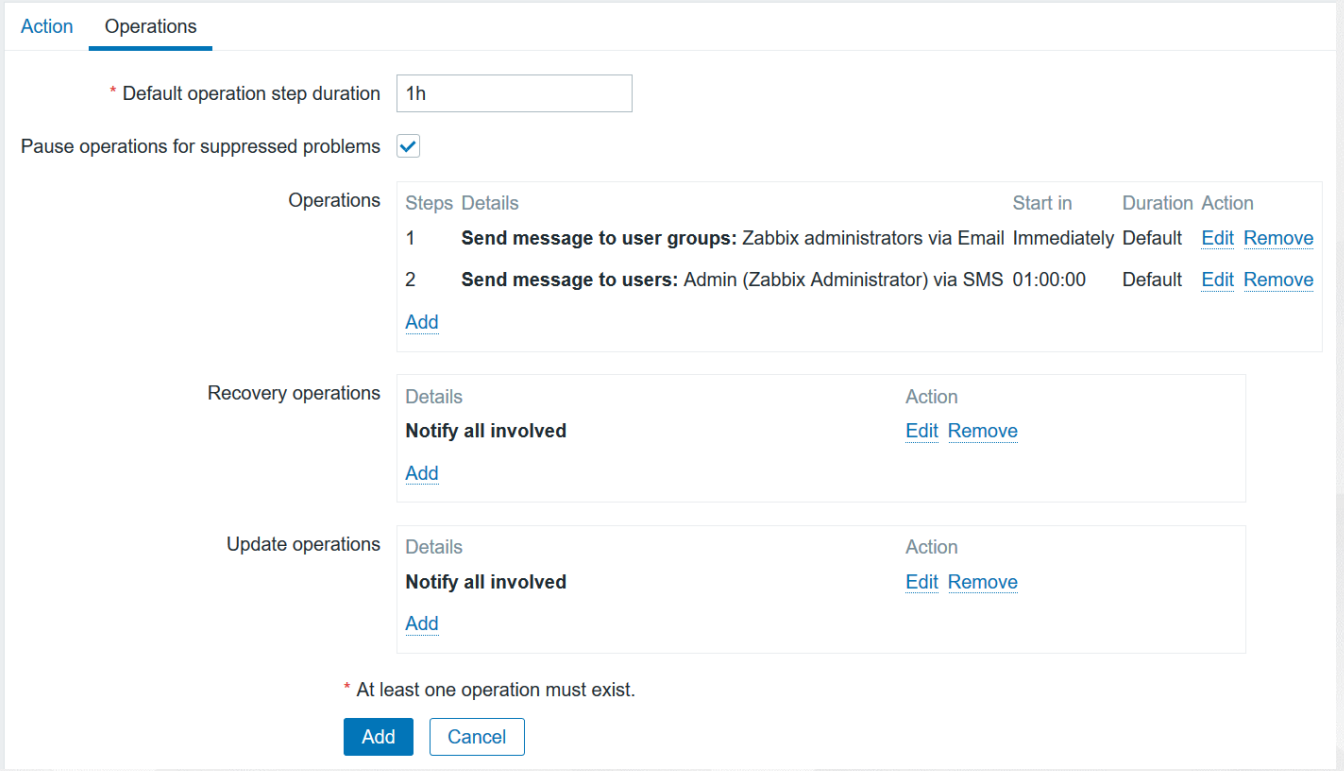




Notifications depend on permissions - no permissions = no notifications

For Trigger actions:

- Operations
- Recovery operations
- Update operations



Default operation step duration:

- 60 seconds to 1 week
- Supports:
  - Time suffixes e.g. 60s, 1m, 2h, 1d
  - User macros

Pause operations for suppressed problems:

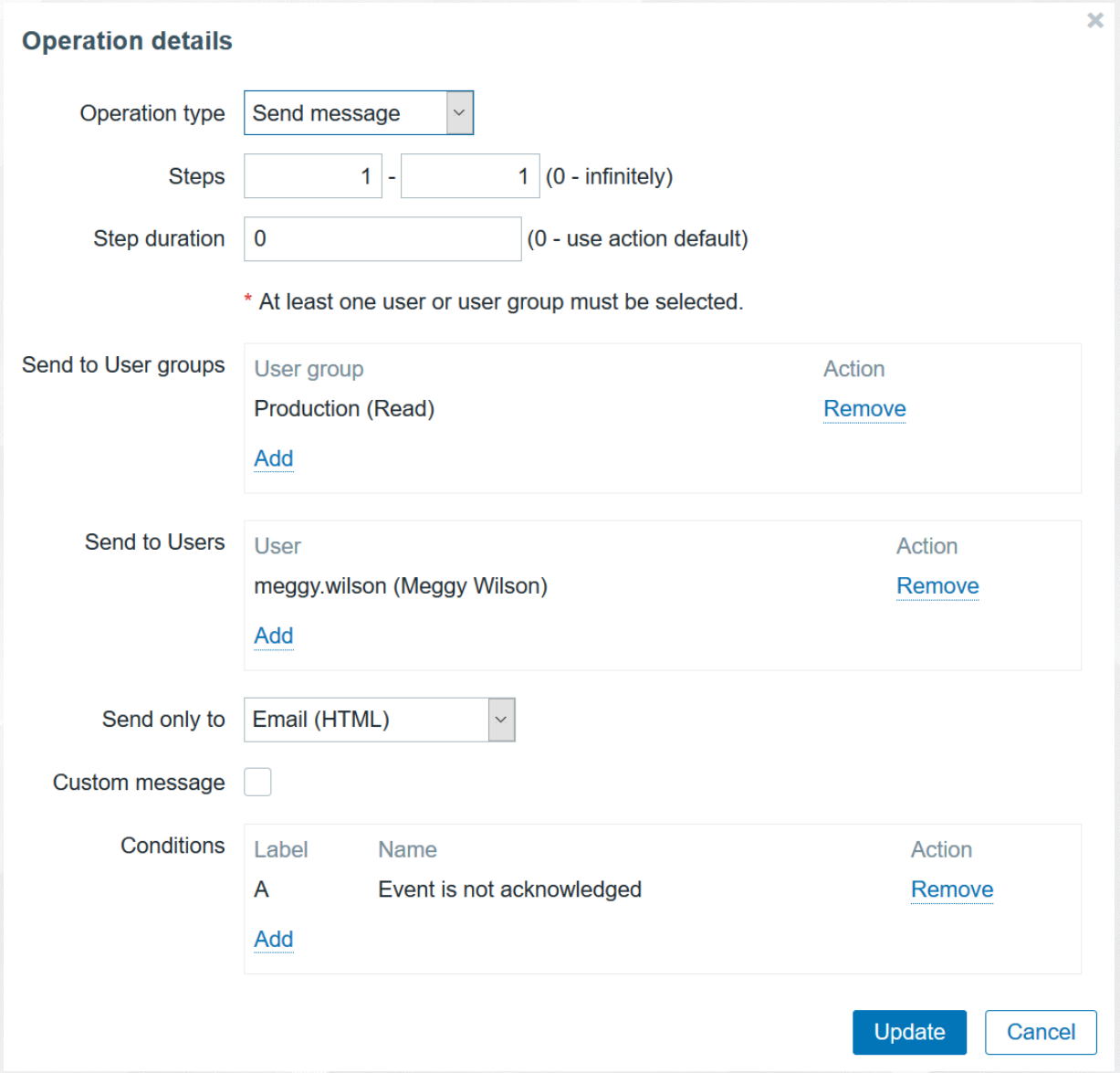
- Delays the start of operations if the event is suppressed
  - Maintenance
  - Trigger dependency

Send message:

- Single user, group
- Single media, all
- Message
- Condition based on acknowledgement

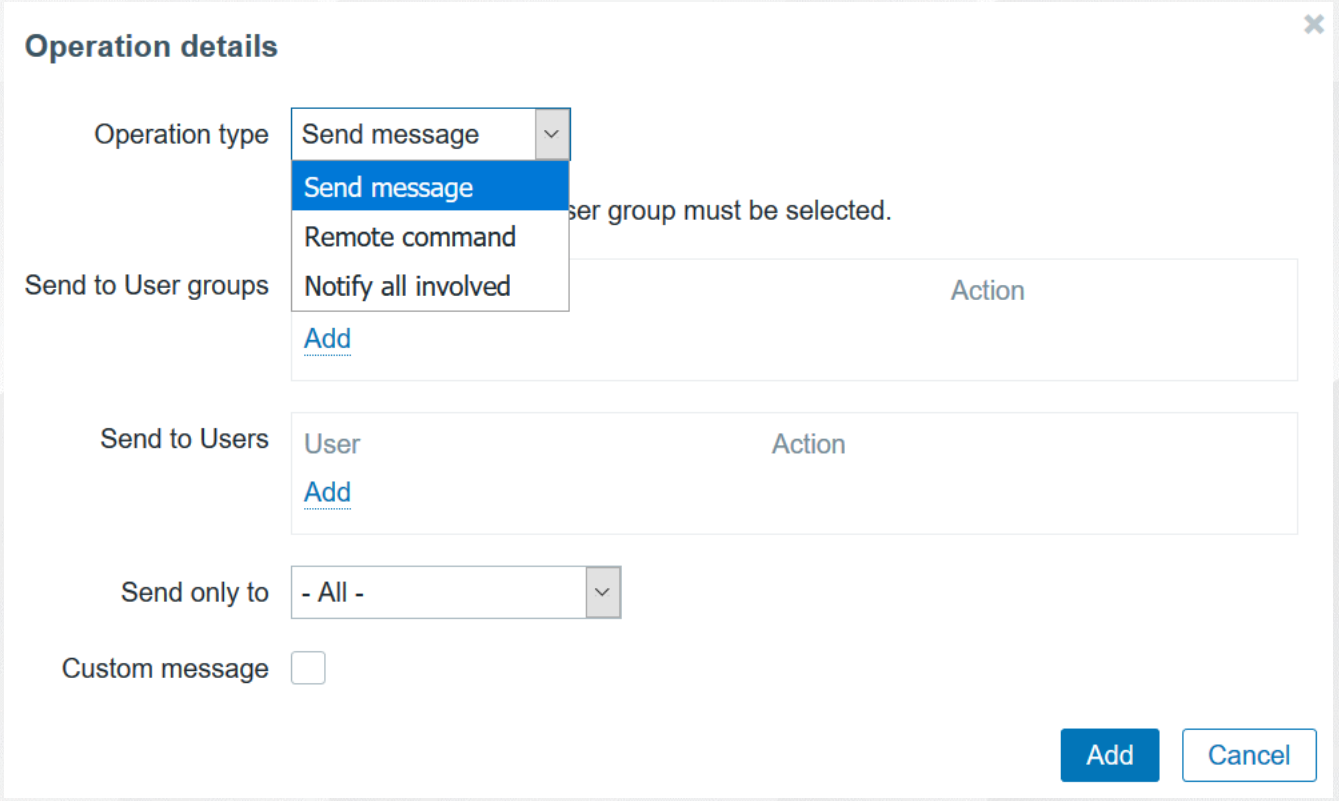
Run remote command:

- On the server or by agent
- IPMI
- SSH, telnet
- Global script



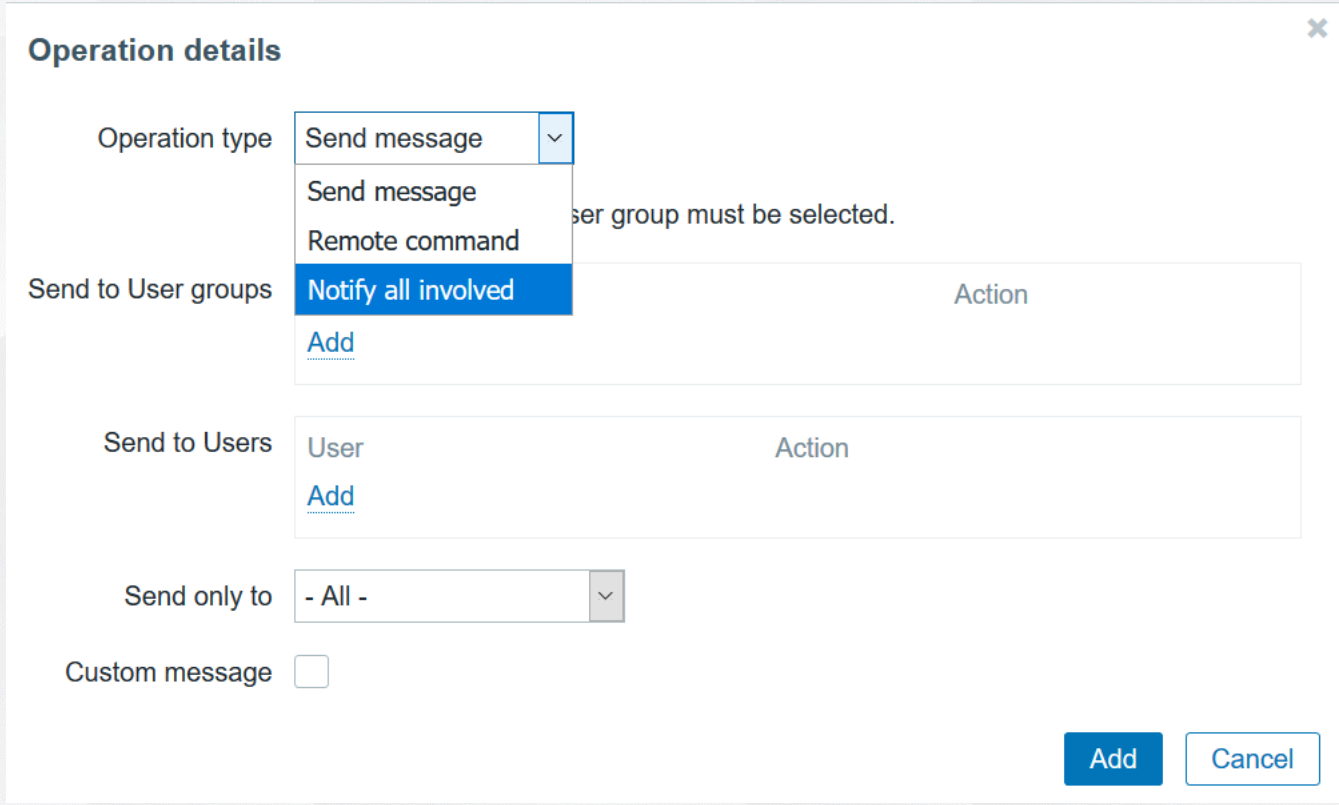
ACTIONS - RECOVERY OPERATIONS

- Recovery operations allow you to be notified when problems are resolved
  - by a trigger going back to OK" state
  - by manually closing a problem
- Both, messages and remote commands, are supported in recovery operations
- Recovery operations do not support escalations - all operations are assigned to a single step

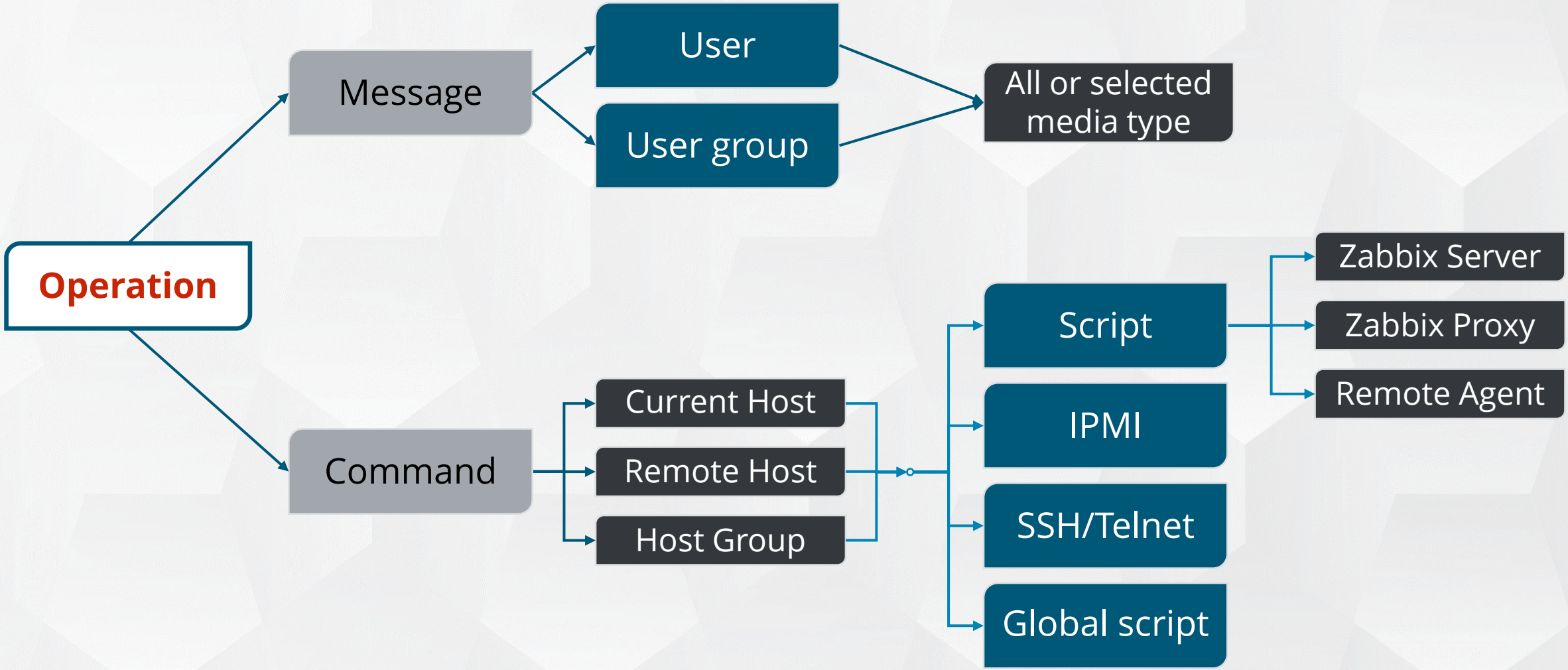


ACTIONS -UPDATE OPERATIONS

- Update operations allow you to be notified when problems are updated. If someone:
  - adds a message to the problem
  - acknowledges the problem
  - changes problem severity
- Both, messages and remote commands, are supported in update operations
- Update operations do not support escalations - all operations are assigned to a single step



ACTIONS - OPERATIONS DIAGRAM



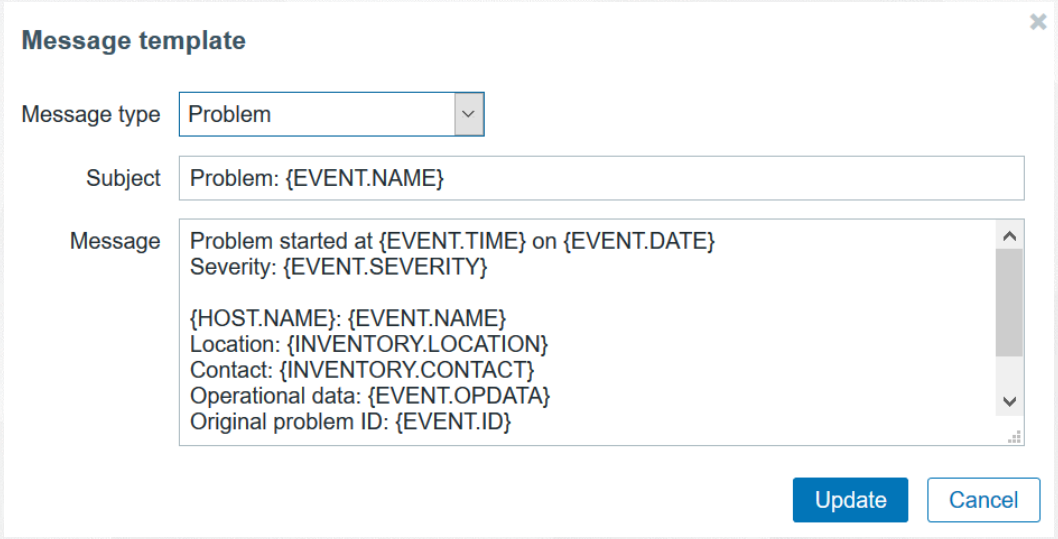
Remote commands must be enabled on Zabbix agent and proxies

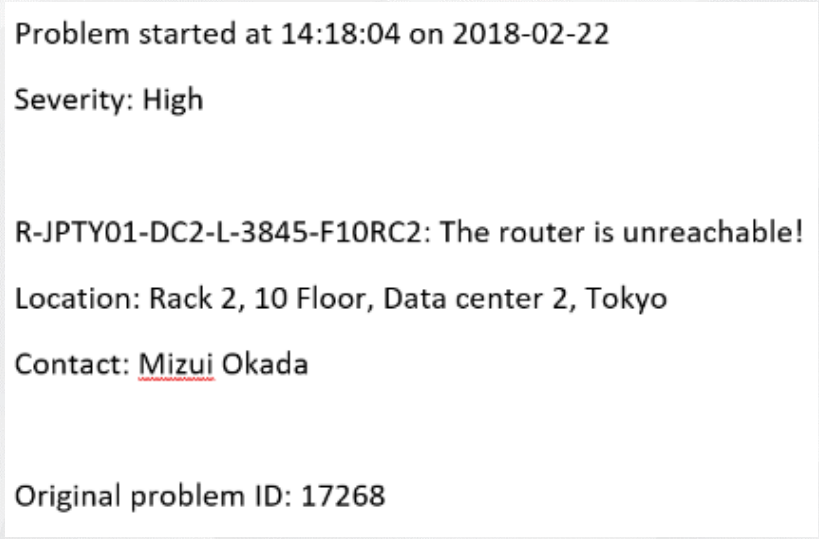
Use macros to include in notifications:

- Technical data such as last gathered value or host details
- Problem details using {EVENT.*} macros
  - The {ESC.HISTORY} macro includes full escalation history
- Host inventory details using {INVENTORY.*} macros

Useful for:

- Providing information without logging in to Zabbix frontend
- Integrations with ticketing systems



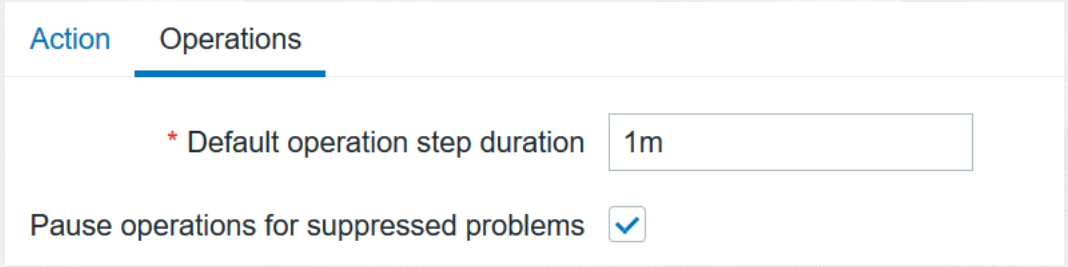


Based on steps

Default interval can be overridden in operations

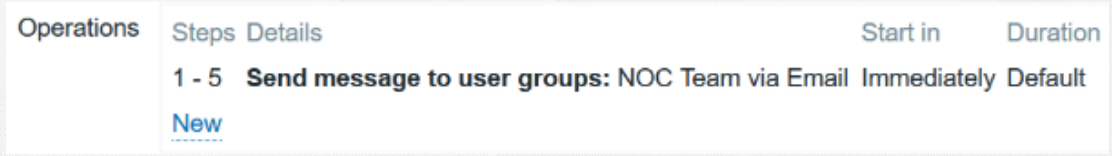
If step intervals collide, the smallest interval wins

1. Duration of every operation step:
   - 1 minute to 1 week
   - Can be overridden in step configuration
   - Suppressed problems can be paused

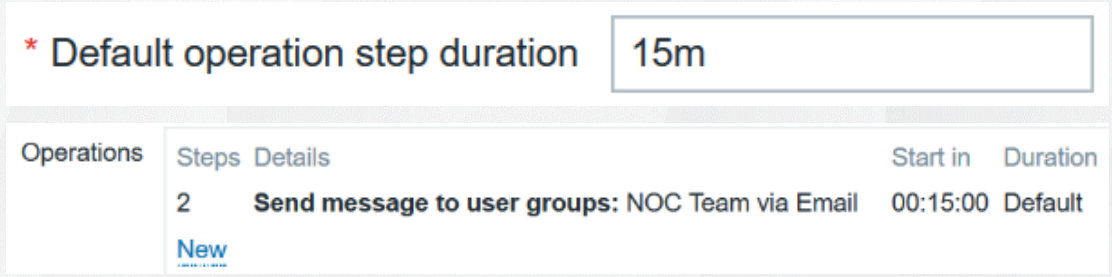


2. Steps:
   - From - execute starting with this step
   - To - execute until this step
   - 0 = infinity, execution will not be limited
   - Custom duration for a single step

- Example 1. Sending a repeated notification once every hour (5 times in total):



- Example 2. Sending a postponed notification:



- Example 3. Escalating the problem after 1 hour to the Boss:

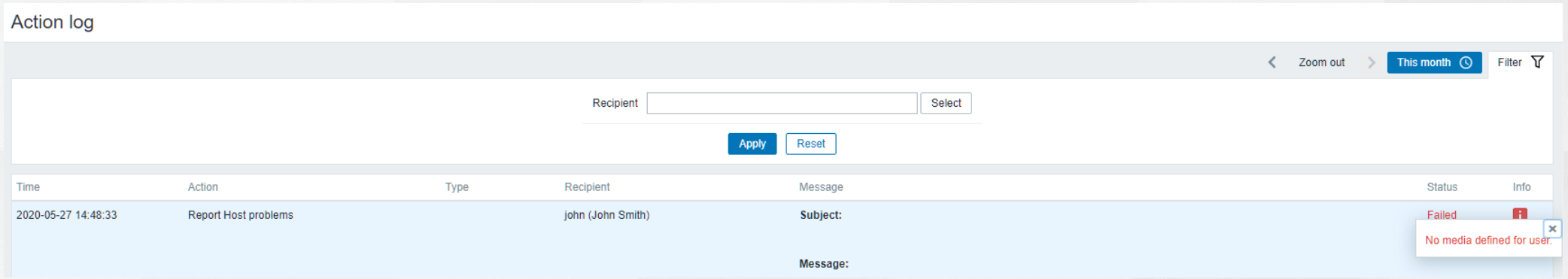
Immediately	email administrator
10 minutes	send SMS to admin
15 minutes	open a report at helpdesk system
30 minutes	email management
1 hour	send SMS to management
2 hours	restart Apache
6 hours	reboot the server
24 hours	power cycle whole server room

ESCALATION BEHAVIOR

Situation **Escalation in progress**	Behavior
Based on any type of event: - the action is disabled - the event is deleted - the trigger is disabled or deleted - the host or item is disabled	The message in progress is sent Another message on the escalation is sent: • "NOTE: Escalation cancelled" • The recipient is informed that escalation is cancelled • No more steps are executed
- action is deleted	• No more messages are sent. • Information is logged to the server log file. Example: "escalation cancelled: action id:555 deleted"

NOTIFICATIONS DO NOT WORK

- Make sure the user has at least read permissions on the host that generated the event
- Verify that both , email settings and action conditions, have been configured properly
- Check user media conditions in user profile
- Check that all media templates are defined
- Check the details by navigating to Monitoring > Problems and clicking on time for the event
- Check action log by navigating to Reports > Action log



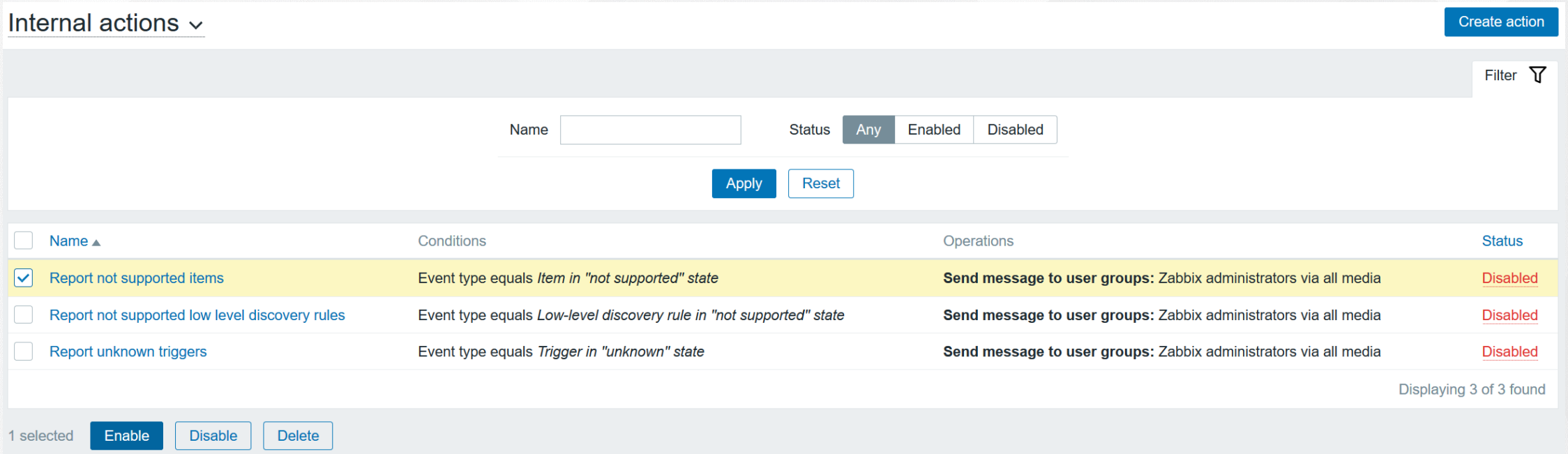
PRACTICAL SETUP

1. Add Email Media type:
   - Name: Training email
   - SMTP server: training.lan
   - SMTP server port: 25
   - SMTP helo: training.lan
   - SMTP email: trainingXX@training.lan
2. Configure your user media - add email address
3. Customize messages
   - Add OS details and location to message body (use inventory fields)
4. Update your user profile - add an email
5. Create an action with 2 steps:
   - send email message immediately in case of a problem
   - execute a command after 1 minute
6. Generate a problem to test notifications (e.g. CPU load is high)

Detection of misconfiguration

Navigate to: Configuration > Actions > Internal actions

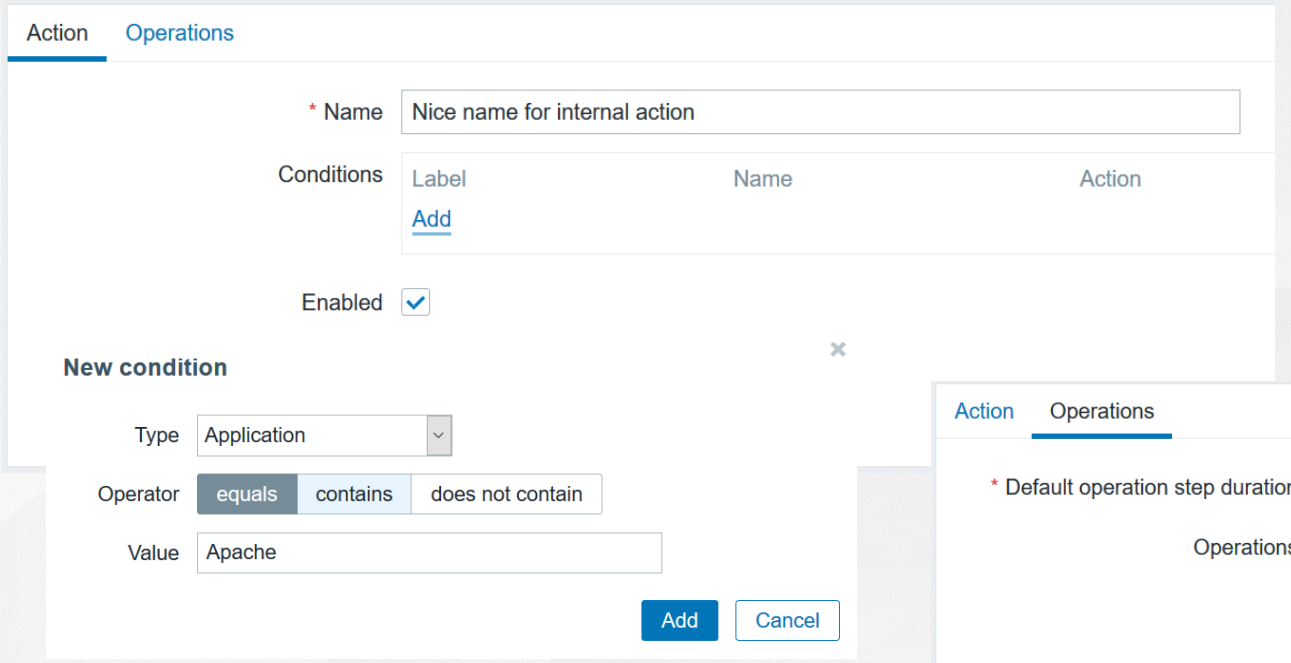
- Detection of problems in configuration:
  - Not supported items
  - Not supported low level discovery rules
  - Unknown triggers

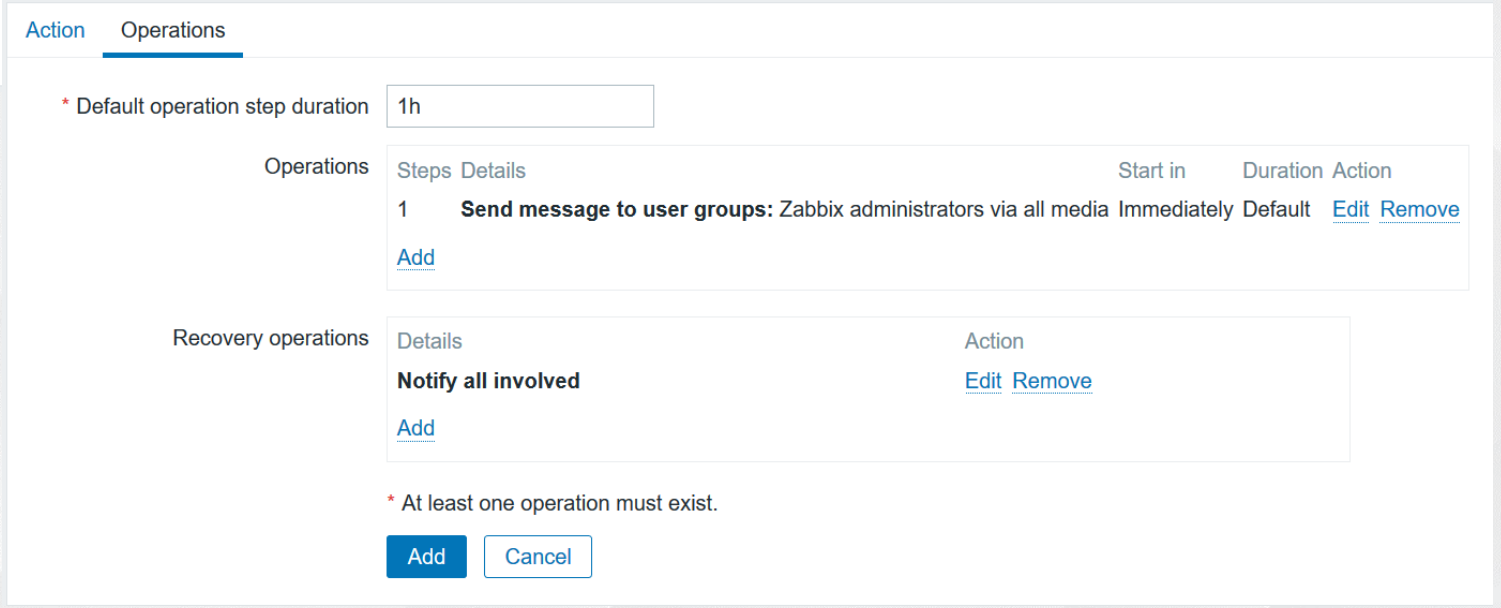


- By default there are three example actions created to report all problems with entities.

Configuration > Actions > Internal actions > [Create action]

Define Conditions and Operations





PRACTICAL SETUP

1. Set up a media type for internal actions:
   - Create a Problem message template
   - Create a Recovery message template
2. Set up an action to report not supported SSH items:
   - Make an SSH item ”Not supported”
   - Check the problem message
   - Make the SSH item supported again
   - Check the recovery message
3. Check reports for actions.

Advanced task: Create internal action for triggers, use tag "Location", test it, break trigger.

Custom notifications

On the Zabbix server side, add a new Media type with type Script

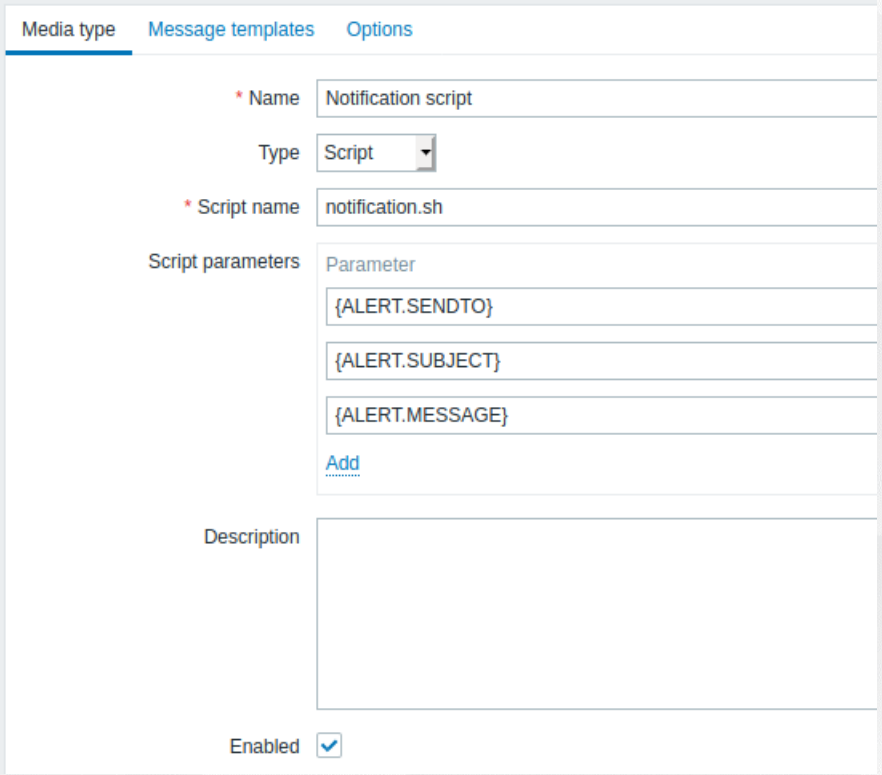
- Script must be located in a directory, specified by AlertScriptsPath directive in zabbix_server.conf

Command-line parameters can be defined per each script

Example:

- {ALERT.SENDTO} – Send to
- {ALERT.SUBJECT} – Subject
- {ALERT.MESSAGE} – Body

Executed by Zabbix server daemon as user "zabbix"



https://www.zabbix.com/documentation/5.0/manual/config/notifications/media/script

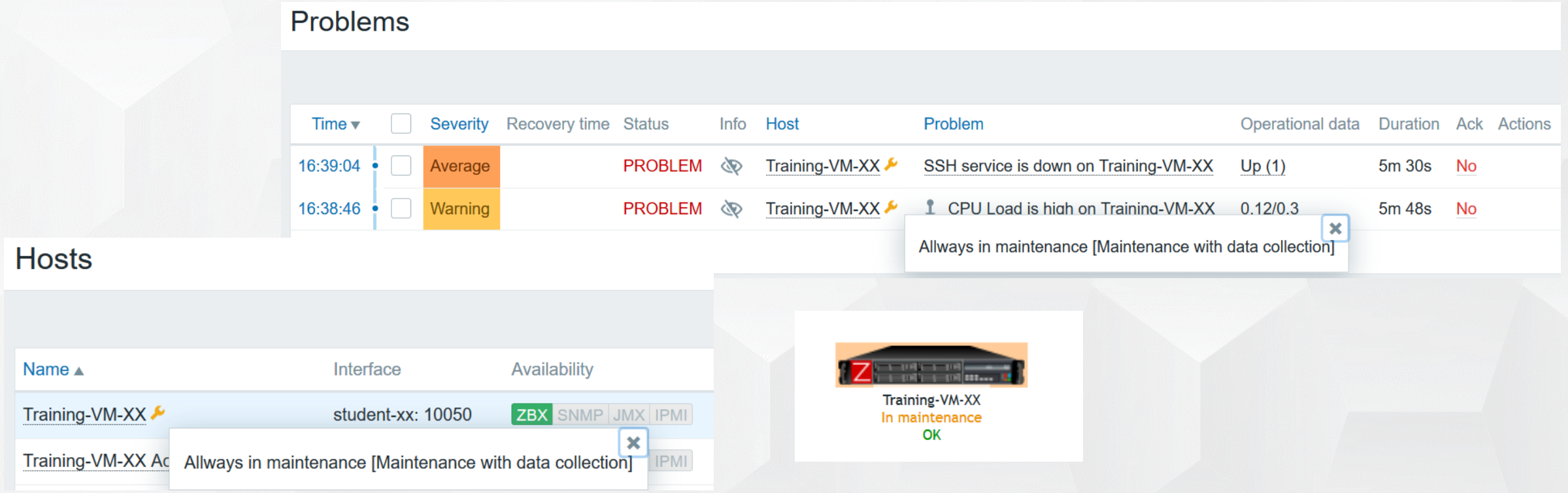
PRACTICAL SETUP

1. Create a script to echo messages to log file:
   - Name: Write to log
     - Send as much information to log as possible, including values from the items
2. Upload script to the server media scripts folder
   - Make script executable
   - Set proper access permissions
3. Create an action to push events to the log file

MAINTENANCE

Maintenance is used to:

- Suppress notifications
- Suppress data collection

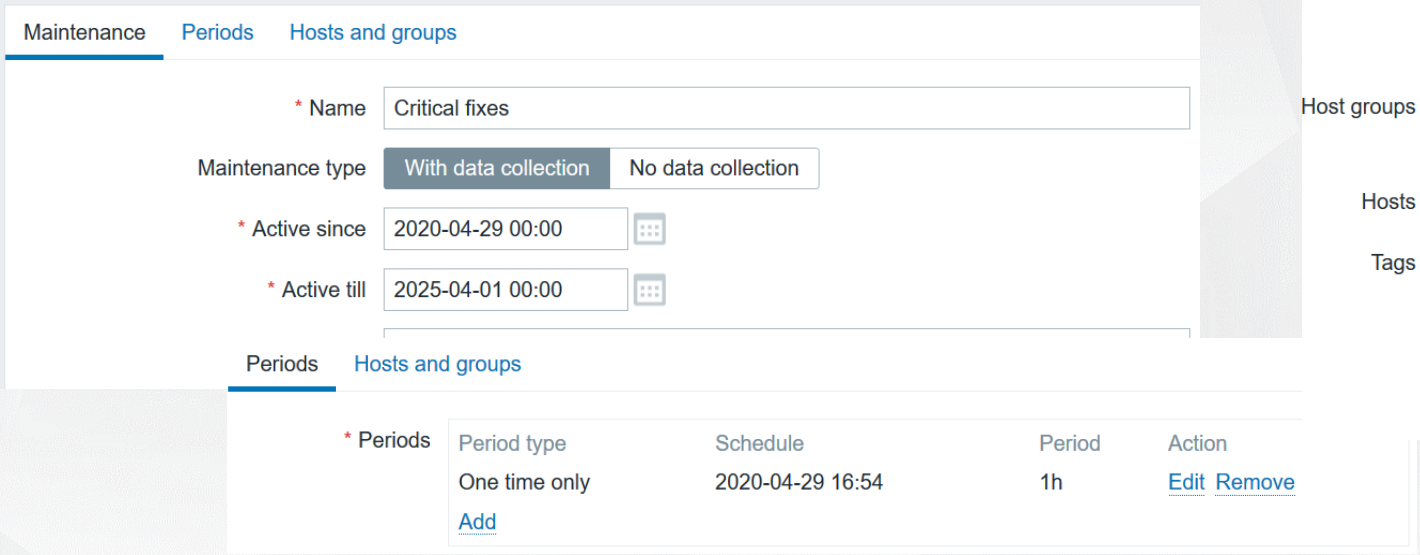


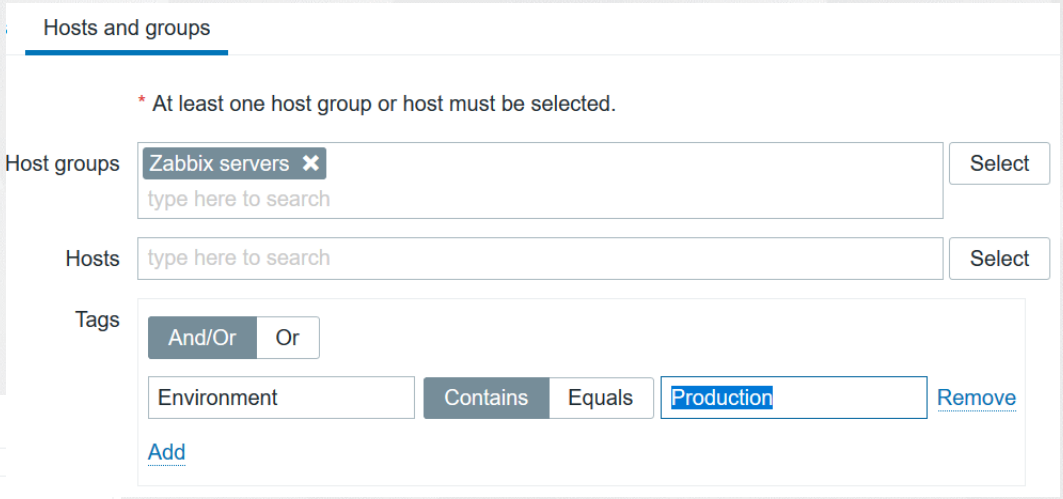
- Visually identified in problems, maps and dashboard, depending on filter settings

https://www.zabbix.com/documentation/5.0/manual/maintenance

MAINTENANCE IN ACTION

- The Timer processes are responsible for switching host status to/from maintenance at 0 seconds of every minute:
  - Maintenance periods for hosts, host groups and problems
  - No maintenance for a specific item, application or template
  - History of maintenance periods is not stored
  - If tags are specified:
    - the hosts will be activated
    - problems will be suppressed if tags match





Periods must be inside the Maintenance rule Active timeframe!

When a host is in maintenance:

- all problems will be suppressed

Time		Severity	Info	Host	Problem
11:59:02 AM	☐	Average		net.brocade.fc.300	FAN #3: Fan is in critical state
11:59:02 AM	☐	High		net.brocade.fc.300	SLOT #1: critical state

If the tags have been specified:

- maintenance for selected hosts will be limited to problems with the corresponding tags

Time		Severity	Info	Host	Problem
11:59:02 AM	☐	Average		net.brocade.fc.300	FAN #3: Fan is in critical state
11:59:02 AM	☐	High		net.brocade.fc.300	SLOT #1: critical state

Workflow:

- Problem > Action executed > Escalator generates steps

Example:

- Simple action with 3 operation steps

Action steps	Operation	Execution time
Step 1	Mail to Admin	immediately
Step 2	Sms to Admin	+10
Step 3	Open ticket in Jira	+20

With maintenance, there are two scenarios:

- A problem starts and the host goes into maintenance
- A host goes into maintenance and a problem starts

Maintenance uses Zabbix server time

A problem starts, but 5 minutes later the host goes into maintenance.

- Maintenance rule:
  - Period 60 minutes
  - From 11:00 till 12:00
- Operation step duration 10 minutes

			Pause operations for suppressed problems			
			Yes		No	
Event	Action steps	Operation	Step timing	Step execution time	Step timing	Step execution time
10:55 Problem	1	Mail to Admin	Immediately	10:55	Immediately	10:55
11:00 Maintenance			**Pause for 60 minutes**			
	2	Sms to Admin	+10 **+60**	12:05	**+10**	11:05
	3	Open ticket in Jira	+20 **+60**	12:15	**+20**	11:15

A host goes into maintenance and the problem starts 10 minutes later

- Maintenance rule:
  - Period 60 minutes
  - From 11:00 till 12:00
- Operation step duration 10 minutes

			Pause operations for suppressed problems			
			Yes		No	
Event	Action steps	Operation	Step timing	Step execution time	Step timing	Step execution time
11:00 Maintenance			**Pause for 60 minutes**			
11:10 Problem	1	Mail to Admin	**+50**	12:00	Immediately	11:10
	2	Sms to Admin	+10 **+50**	12:10	**+10**	11:20
	3	Open ticket in Jira	+20 **+50**	12:20	**+20**	11:30

PRACTICAL SETUP

1. Create a new maintenance:
   - Name: Training maintenance
2. Configure new maintenance period for your host:
   - Period type: One time only
   - Date: today as soon as possible
   - Maintenance period length: 1 hour
3. Check frontend for maintenance status (orange background/wrench icon).

Advanced task: Create another daily maintenance by using Tags

Business level monitoring

Define your SLAs

- Understand business-level impacts and set reasonable targets
- Translate business-level SLAs to component SLAs

Measure your SLAs

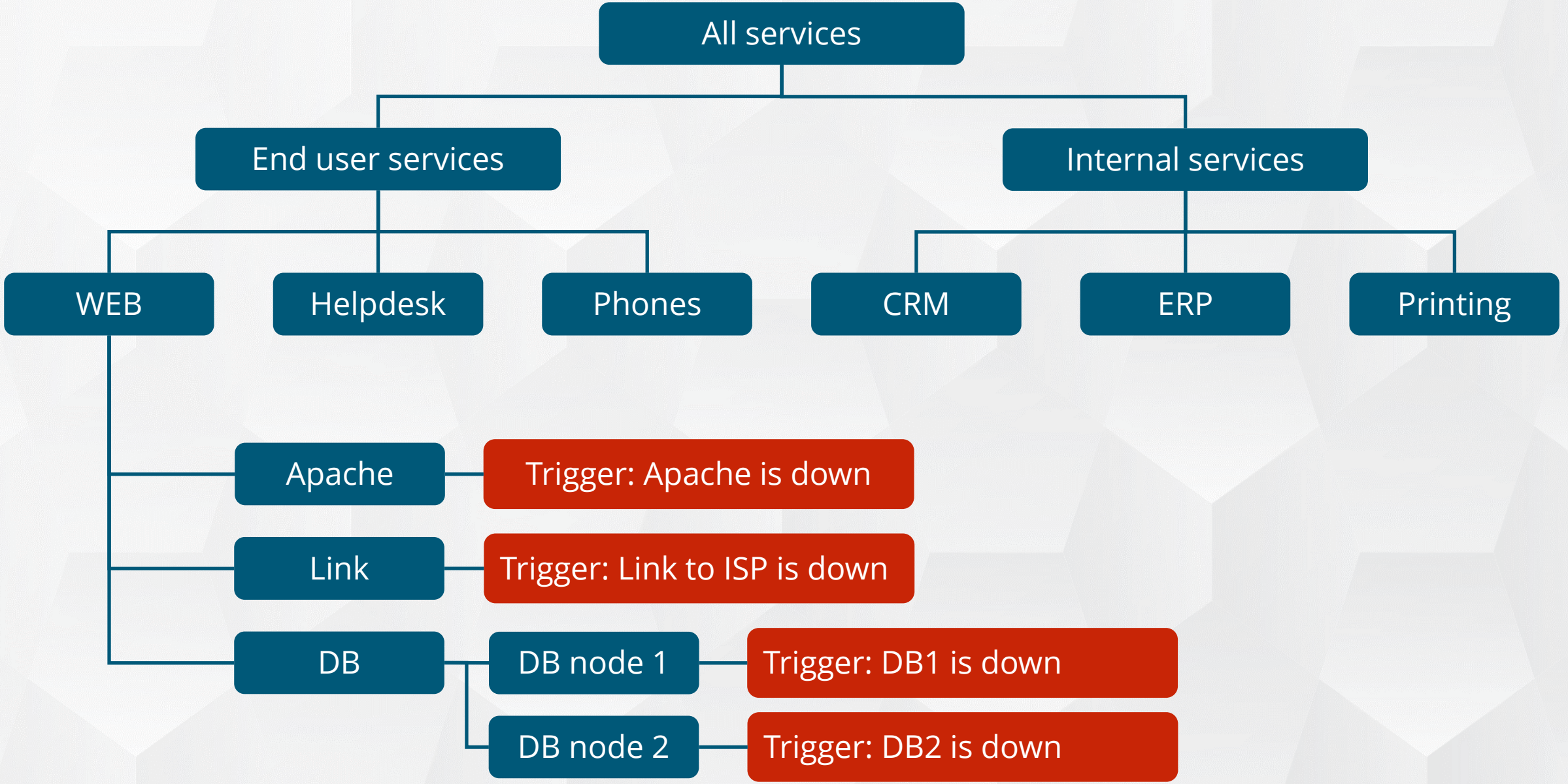
- Service/application monitoring
- Middleware (App server, JMX, ODBC)
- Log files
- Host/OS level monitoring

Configuration > Services

- Parent-child relationship
- Linked to triggers, problem if all/any child has a problem
- Optional SLA calculation per service

SERVICE	ACTION	STATUS CALCULATION	TRIGGER
root	Add child		
▼ Card system	Add child	Problem, if at least one child has a problem	
▶ Application	Add child	Problem, if all children have problems	
▶ Middleware	Add child	Problem, if at least one child has a problem	
▶ Infrastracture	Add child	Problem, if at least one child has a problem	
▼ Channels	Add child	Problem, if at least one child has a problem	
▼ Riga office	Add child	Problem, if all children have problems	
iNet	Add child Delete	Problem, if at least one child has a problem	Incoming traffic for Provider eth2 (10.0.2.15) is too low
Baltic	Add child Delete	Problem, if at least one child has a problem	Incoming traffic for Provider eth3 (192.168.56.30) is too low
▶ Tokyo office	Add child	Problem, if all children have problems	
▶ Providers	Add child	Problem, if at least one child has a problem	

BUSINESS LEVEL MONITORING - SLA



Monitoring > Services

- SLA displaying
- SLA graphs
- Can't be calculated retroactively
- "Not classified" and "Information" severity triggers are ignored for SLA calculation!

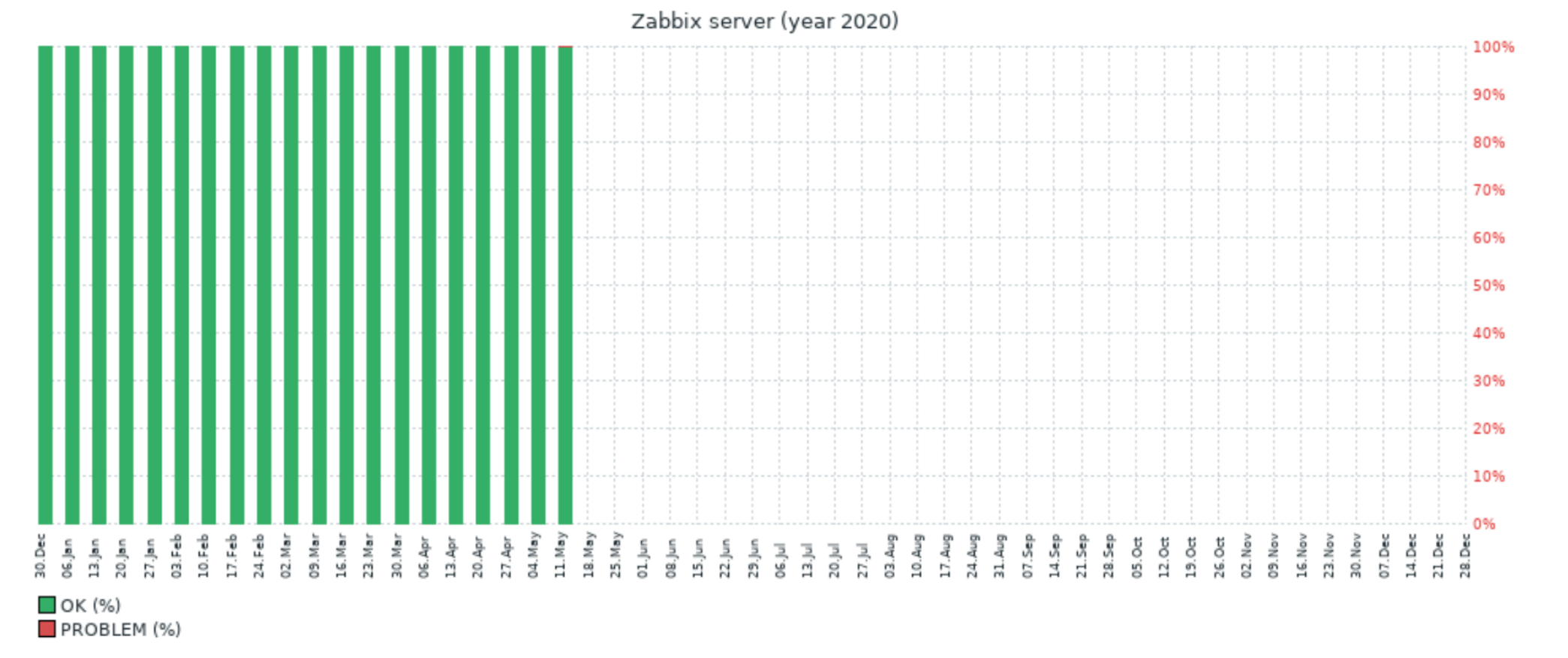
Services

Period: Last 7 days

Service	Status	Reason	Problem time	SLA / Acceptable SLA
root				
▼ Zabbix server	Average	High memory utilization (>90% for 5m)	0.0885	99.9115 / 99.5000
▼ Database	OK		0.0000	100.0000 / 99.5000
MySQL	OK			
▼ Frontend	OK		0.0000	100.0000 / 99.5000
Apache	OK			
PHP fpm	OK			
▼ Zabbix server daemon	Average	High memory utilization (>90% for 5m)	0.0885	99.9115 / 99.5000
Caches - High memory utilization (>90% for 5m)	Average	High memory utilization (>90% for 5m)		

Weekly based.

Shows only problem/OK states



Daily / Weekly / Monthly / Yearly

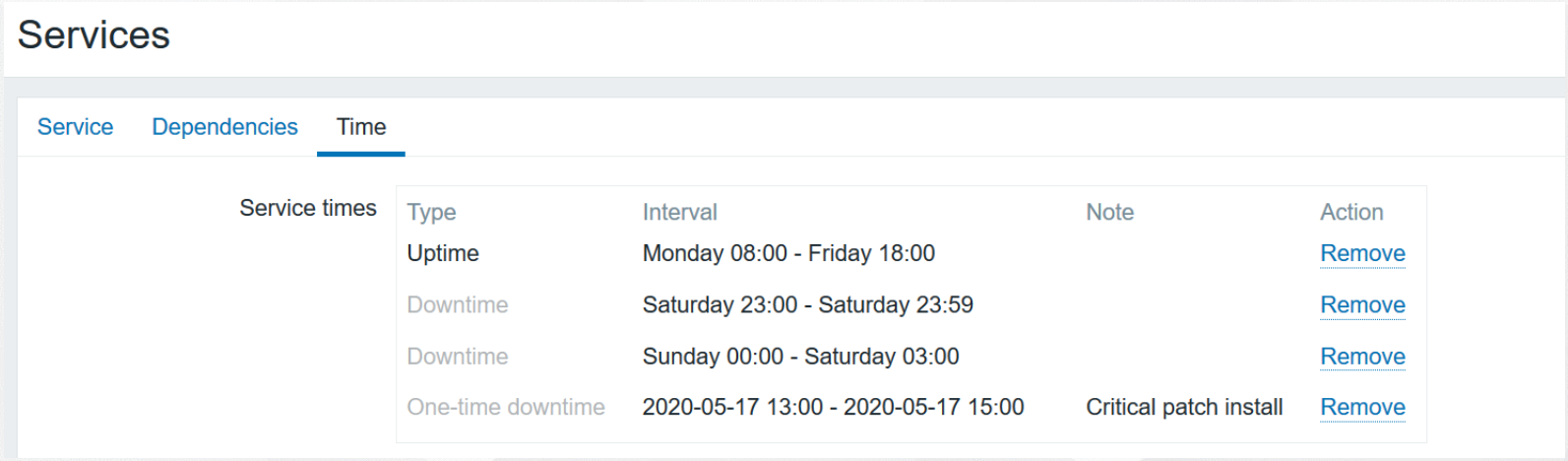
Service availability report: Zabbix server

Period Weekly Year 2020

From	Till	Ok	Problems	Downtime	SLA	Acceptable SLA
2020-05-11 00:00	2020-05-16 12:17	5d 12h 3m	0d 0h 13m		99.8299	99.5
2020-05-04 00:00	2020-05-11 00:00	7d 0h 0m			100.0000	99.5
2020-04-27 00:00	2020-05-04 00:00	7d 0h 0m			100.0000	99.5
2020-04-20 00:00	2020-04-27 00:00	7d 0h 0m			100.0000	99.5
2020-04-13 00:00	2020-04-20 00:00	7d 0h 0m			100.0000	99.5
2020-04-06 00:00	2020-04-13 00:00	7d 0h 0m			100.0000	99.5

Every service has its own time settings:

- Uptime - service uptime
- Downtime - service state within this period does not affect SLA
- One-time downtime - a single downtime
  - Service state within this period does not affect SLA
- Service times affect calculation of service status and SLA by the frontend
- The "No data collection" maintenance can be used to configure the maintenance period for a service (no data = no problems = no downtime)



PRACTICAL SETUP

1. Create a new SLA:
   - Name: Zabbix training SLA
   - Acceptable SLA 95%
   - Status calculating algorithm: Problem if at least one child has a problem
   - Add training schedule including lunchtime for every day as Uptime/Downtime
2. Children: you and 2 other trainees(example : student-XX)
   - Add a trigger: CPU Load is very high on {HOST.NAME}
3. Make the triggers switch to problem state
4. Check service counters

Low-Level Discovery

Low-level discovery provides a way to automatically create:

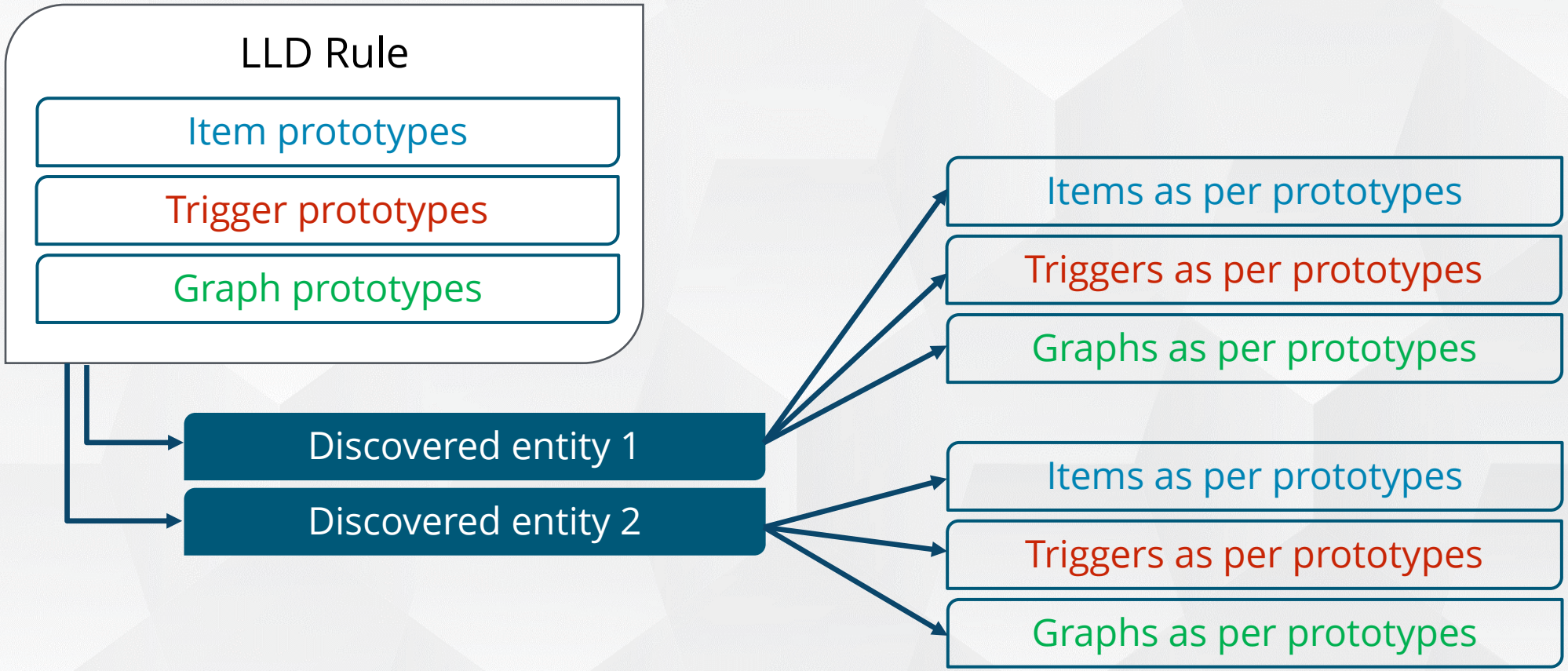
- Items
- Triggers
- Graphs
- Screens
- Hosts

- Automatically start monitoring file systems, network interfaces and other things.
- No need to create items manually – prototypes are used
- Possible to remove unneeded entities automatically

https://www.zabbix.com/documentation/5.0/manual/discovery/low_level_discovery

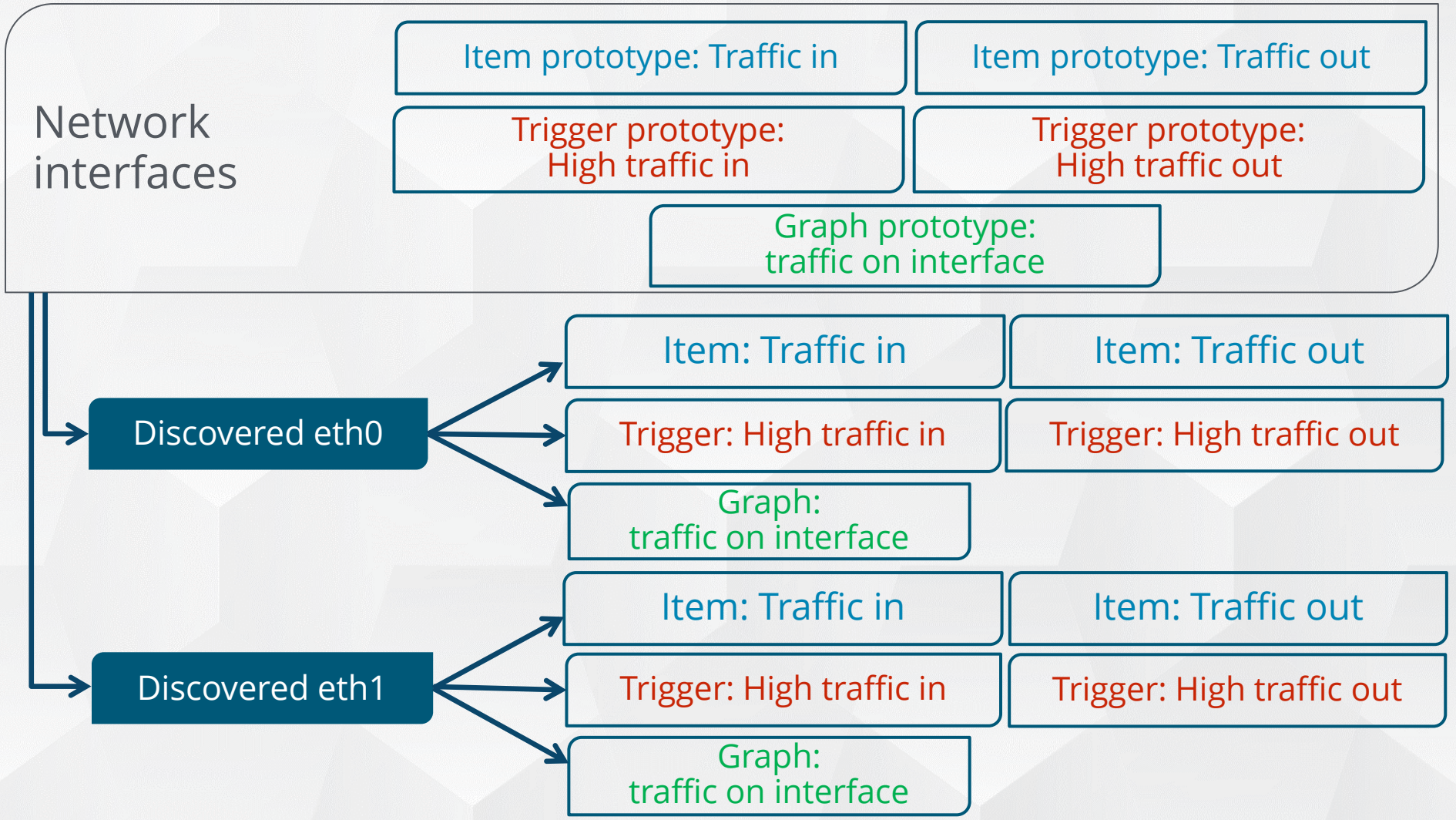
Workflow:

- Create discovery item/rule in Configuration > Templates > Discovery
- Create prototypes of items, triggers and graphs that should be created by the rule



This topic is discussed in Professional and Expert level training

Example of the network interface discovery:



LOW-LEVEL DISCOVERY(LLD) - BUILT-IN ENTITIES

- Zabbix agent
  - Filesystems
  - Block devices
  - Network interfaces
  - CPUs and CPU cores
  - Only on Windows
    - Services
    - WMI queries
    - Performance counters
- Linux systemd services (only for Agent2)
- SNMP entities
- JMX entities
- IPMI entities
- SQL entities
- Zabbix host interfaces
- ...anything using scripting

PRACTICAL SETUP

1. Use host: Training-VM-XX
   - Link to template "Template Module Linux filesystems by Zabbix agent"
   - Reload server configuration cache
   - Manually execute the discovery rule
   - Check for automatically created items and values for existing filesystems

2. Check that discovery rule is working as expected
   - Create new virtual filesystem
   - Manually execute the discovery rule
   - Check for automatically created items for new filesystem

Advanced task: Link "Template Module Linux network interfaces by Zabbix agent" check

XML IMPORT/EXPORT

XML IMPORT/EXPORT FUNCTIONALITY

Exports

Hosts and templates:

- Items
- Triggers
- Graphs
- Template linkage
- Host macros
- Applications
- Screens
- WEB scenarios
- Value maps used by items

Value mapping

Media types

Screens

Network maps

- Images are exported in base64 format
- Hosts must be exported separately

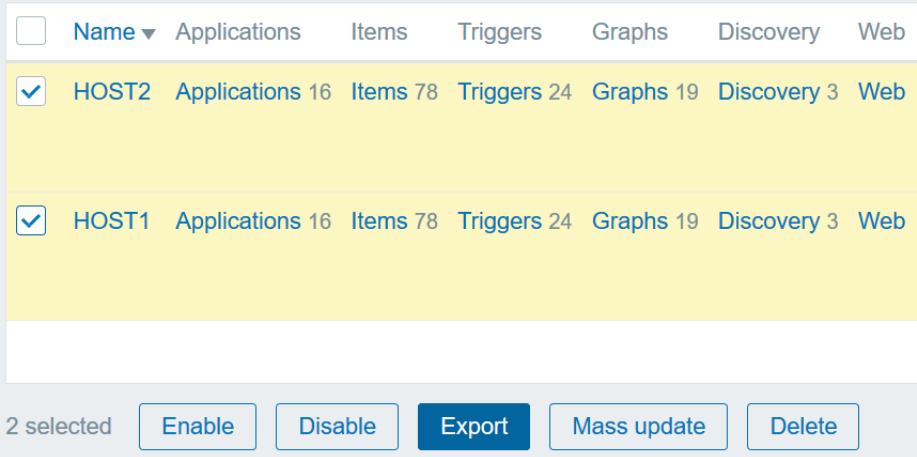
Supports XML exports from previous Zabbix releases 4.X, 3.X, 2.X and 1.8

Values of "Secret text" macros are not exported!

https://www.zabbix.com/documentation/current/manual/xml_export_import

Configuration > Hosts/Templates > Select hosts > [Export]

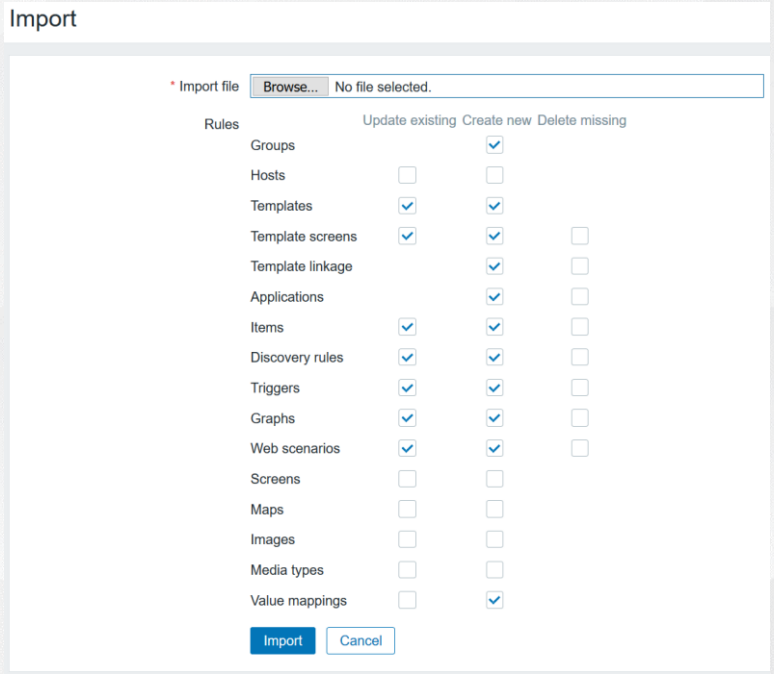
- Partial configuration backup purposes
- Automated/scripted configuration generation
- Scripted large-scale configuration changes
- Configuration transfer from development machine to production



Configuration > Hosts/Templates > [Import]

Global import form

Rule	Description
Update existing	Existing elements will be updated with data taken from the import file. Otherwise, they will not be updated.
Create new	Import will add new elements using data from the import file. Otherwise, it will not add them.
Delete missing	Import will remove existing elements not present in the import file. Otherwise, it will not remove them. If Delete missing is marked for template linkage, existing template linkage not present in the import file will be removed from the host along with all entities inherited from the potentially unlinked templates (items, triggers, etc).



XML IMPORT/EXPORT - EXAMPLE

```
<?xml version="1.0" encoding="UTF-8"?>
<zabbix_export>
    <version>5.0</version>
    <date>2020-04-22T07:47:33Z</date>
    <groups>
        <group>
            <name>Discovered hosts</name>
        </group>
        <group>
            <name>Zabbix servers</name>
        </group>
    </groups>
    <hosts>
        <host>
            <host>Zabbix server 1</host>
            <name>Main Zabbix server</name>
            <proxy>
                <name>Remote proxy</name>
            </proxy>
            <tls_connect>TLS_PSK</tls_connect>
            <tls_accept>
                <option>NO_ENCRYPTION</option>
                <option>TLS_PSK</option>
            </tls_accept>
            <tls_psk_identity>z112</tls_psk_identity>
            <tls_psk>1f87b595725ac58dd977beef14b97461a7c1045b9a1c963065002c5473194952</tls_psk>
            <templates>
                <template>
                    <name>Template App Zabbix Server</name>
                </template>
```

PRACTICAL SETUP

1. Export:
   - Your training host
2. Modify XML file and add:
   - Change: Hostname to trainers VM
   - Visible name: Use trainers name + VM
   - Interface: Use "trainer" as DNS name
3. Import modified XML files back

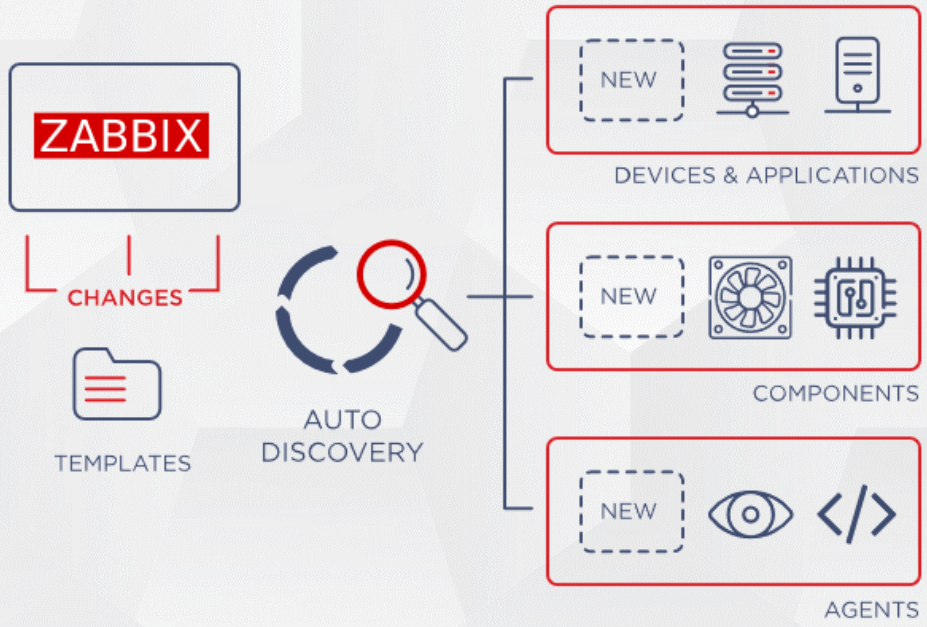
Advanced task: Add a description for trainer's host in XML file.

Automation

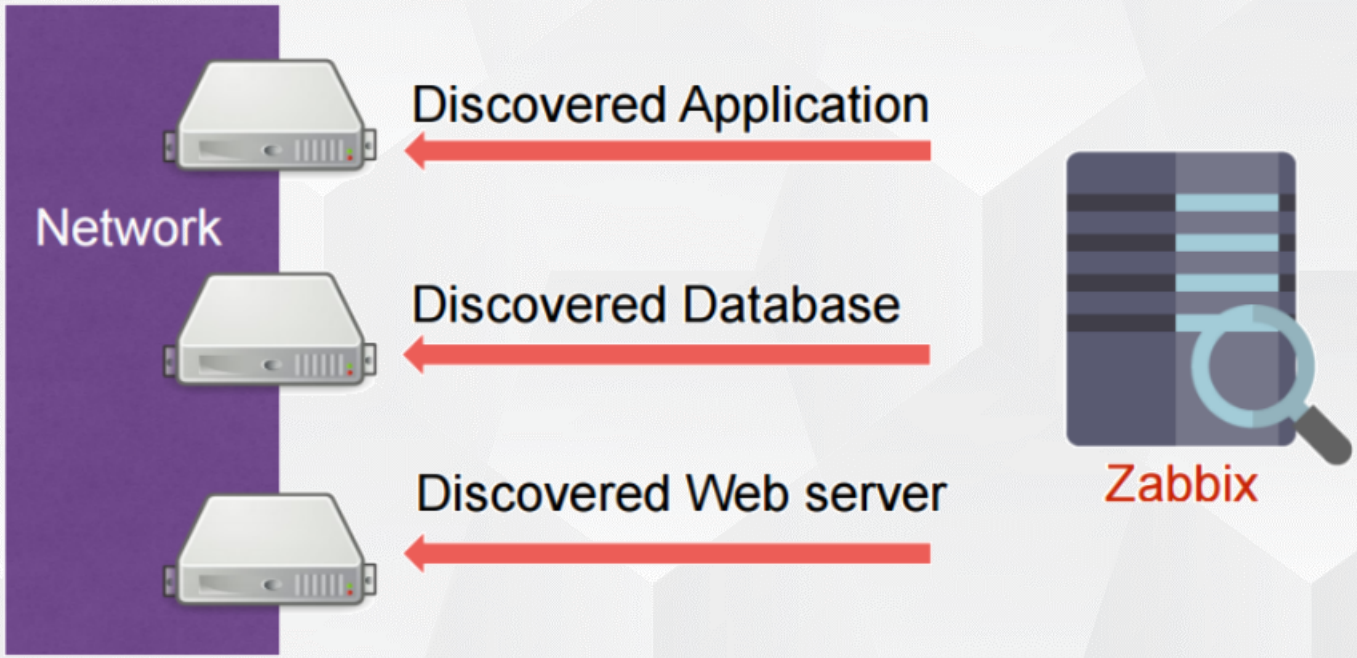
Automate actions for different elements (hosts, applications, etc.):

- Add/remove
- Enable/disable
- Link/unlink templates
- Change groups
- Etc.

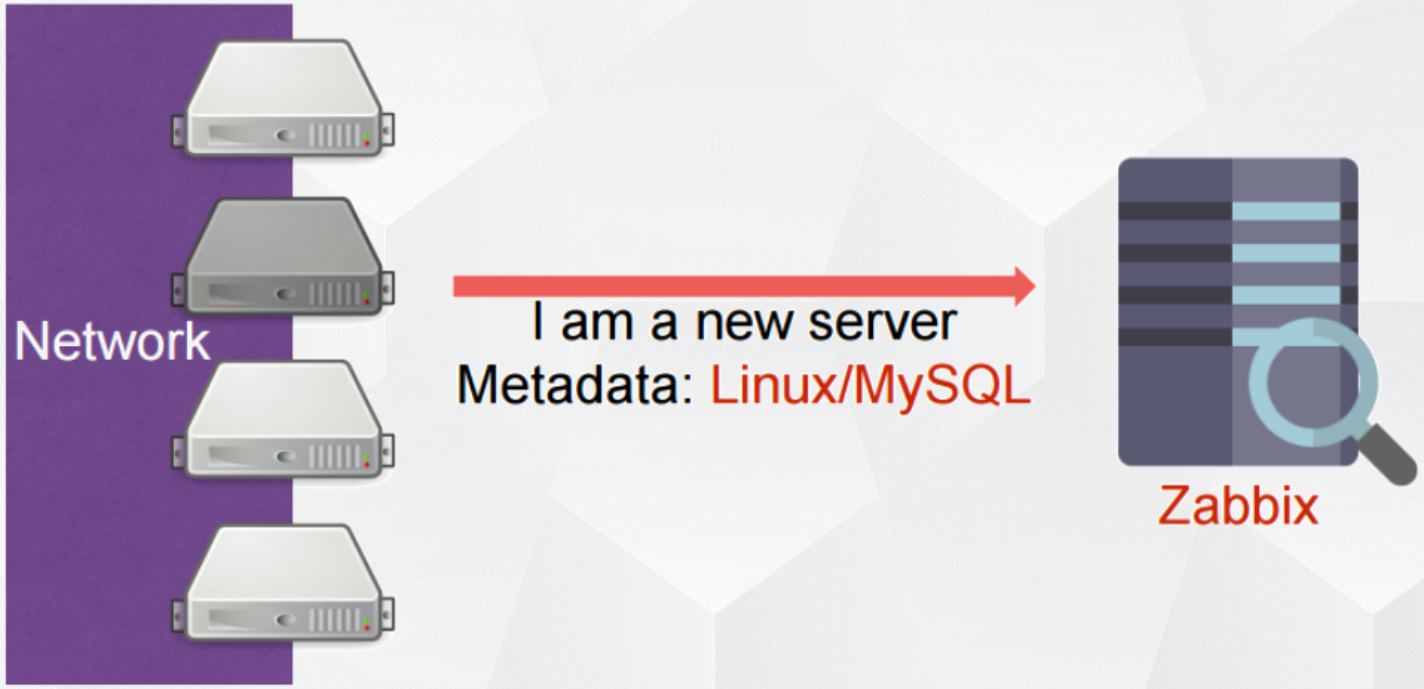
- Auto-registration of active agent
- Network discovery
- Low-level discovery
- Zabbix API



Scan the network for services or devices and take pre-defined actions

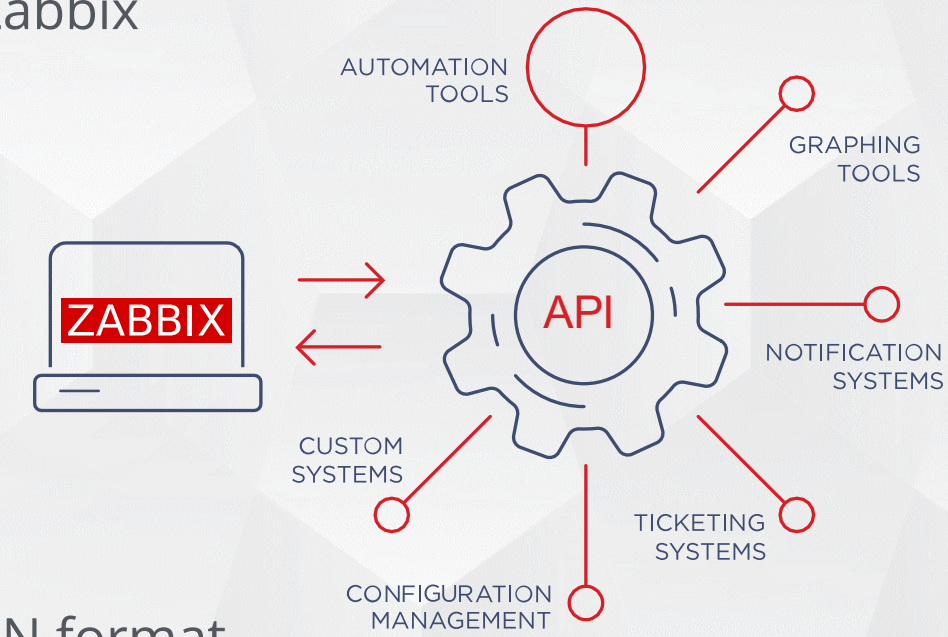


Add new hosts with installed Zabbix agent in active mode for monitoring without any manual configuration



Zabbix API

- Web based and is shipped as part of web frontend
- Allows to retrieve and modify the configuration of Zabbix
- Provides access to historical data
- 230+ different API methods
- Create new applications to work with Zabbix
- Integrate with third party software
- Custom reports
- Respects permissions
- Requests and responses are encoded using the JSON format



BACKUPS

We strongly recommend that you always maintain regular backups as well as make a fresh backup before every upgrade.

- Database backup
- Historical data can be separated: history*, trends*, events*

Configuration files:

- zabbix_server.conf, zabbix_agentd.conf, zabbix_proxy.conf

Scripts, modules, alert and external scripts.

Optional:

- Binaries, frontend files

There are various ways to backup Zabbix DB.

Example for MySQL:

- xtrabackup/mariadbbackup (full physical backup)
- xtrabackup/mariadbbackup (incremental physical backup)
- mysqldump (logical backup)
- binary logging
- replication

The mysqldump is the most popular MySQL backup method.

- safe, but slow (e.g. 100GB/1 hour)
- may cause performance degradation

Xtra/mariadb backup has more recovery options and better performance.

The commands to backup/restore will vary depending on your database and selected backup method

Zabbix database backup:

- PostgreSQL: pg_dump zabbix > zabbix_db
- MySQL: mysqldump --single-transaction -p --tab /mnt/backup zabbix

Restore a backup:

- PostgreSQL: psql zabbix < zabbix_db
- MySQL: cat /mnt/backup/*.sql | mysql -p zabbix
- mysqlimport -p --use-threads=4 zabbix /mnt/backup/*.txt

XML export can be used for other objects in Zabbix, for example, templates or hosts.

MYSQL IMPORT/EXPORT TIPS

Default MySQL settings could cost you 10x restore slowdown.

InnoDB log file size and buffer pool size are important.

When importing data, you can speed up table imports by temporarily turning off the uniqueness checks:

- unique_checks=0
- foreign_key_checks=0
- innodb_doublewrite=0
- sql_log_bin=0

Load files in parallel using N threads.

Restore operation takes more time than the backup.

QUESTIONS?

Time for a break :)