

The ZABBIX logo consists of the word "ZABBIX" in a bold, white, sans-serif font, centered within a solid red rectangular background. The background of the entire slide is a dark blue gradient with a faint, glowing network of white lines and dots, and a semi-transparent world map in the center-right.

ZABBIX

Audit

Artjoms Rimdjons

C Developer

Overview

In 5.0 there is already an Audit

- ZBXNEXT-6470 improves it
- Goal - to audit all configuration and settings changes.
- Who, when and what.
- Enterprise-level requirement.
- Front-end development ongoing
- Server side is mostly done in 6.0
- 7.0 has improvements



Before 6.0...

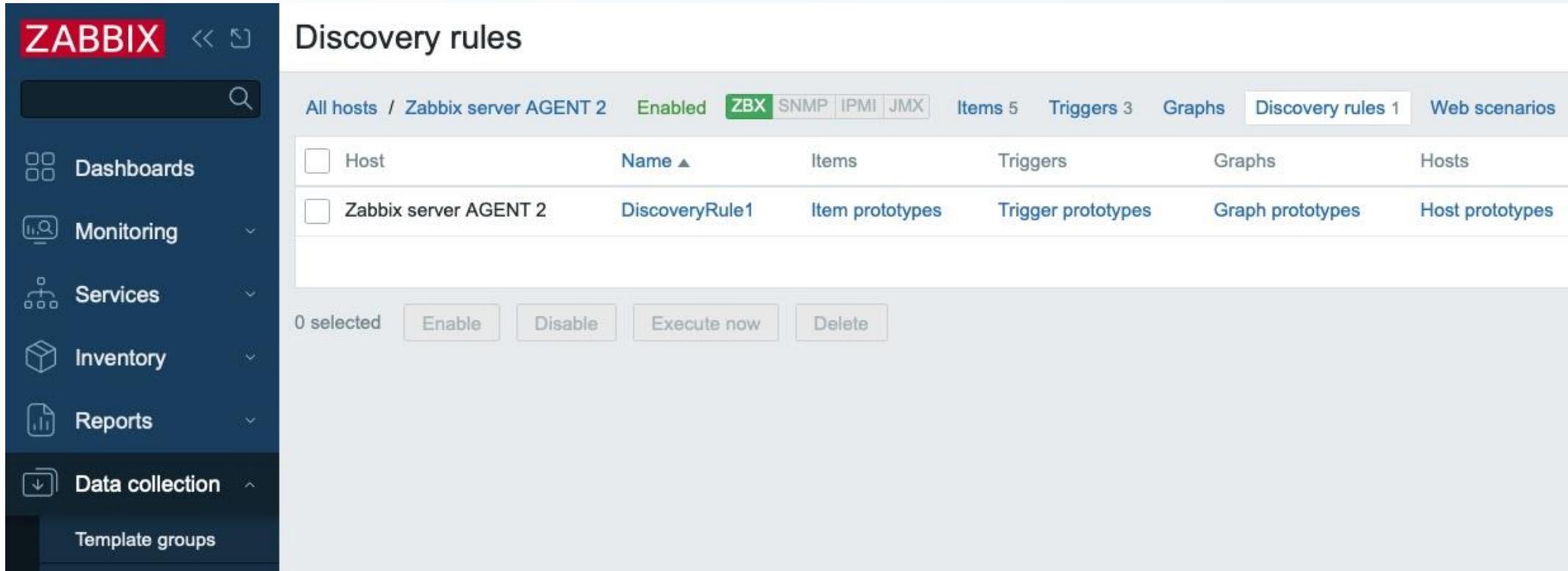
The screenshot shows the Zabbix web interface with the 'Audit log' section selected. The table contains the following data:

Time	User	IP	Resource	Action	ID	Description	Details
2024-04-23 08:11:43	Admin	192.168.64.1	Host	Add	10439	HOST_2	
2024-04-23 08:10:34	Admin	192.168.64.1	Trigger	Add	20118	BADGER_2	
2024-04-23 08:10:03	Admin	192.168.64.1	Template	Add	10438	X	
2024-04-23 08:09:44	Admin	192.168.64.1	User	Add	3	USER2	
2024-04-23 08:09:12	Admin	192.168.64.1	Script	Execute	2		script.execute_on: => 2 script.hostid: => 10084 script.command: => /usr script.output: => traceroute ms
2024-04-23 07:36:24	Admin	192.168.64.1	User	Login	0		

- Zabbix Server may do a lot of configuration yet there is no any audit of that. For example, if host is created on server – nothing is recorded.
- Adding of template on a host – is audited, but no info of items, triggers, tags etc. is present.

Autoregistration and Network Discovery

The screenshot displays the Zabbix web interface for configuring autoregistration actions. The left sidebar contains navigation options: Dashboards, Monitoring, Services, Inventory, Reports, Data collection, Alerts, Actions, Media types, Scripts, and Users. The main content area is titled 'Autoregistration actions' and features a 'New action' section with tabs for 'Action' and 'Operations'. The 'Operations' tab is selected, showing a table with columns for 'Action' and 'Operations'. A dropdown menu is open for the 'Operation' field, listing the following options: Send message, Add host, Remove host, Add to host group, Remove from host group, Link template, Unlink template, Add host tags, Remove host tags, Enable host, Disable host, and Set host inventory mode. The background interface includes a search bar, a table with '0 selected' items, and buttons for 'Enable', 'Disable', and 'Delete'. A modal window titled 'Operation details' is also visible, containing a 'Send to user groups' field with a 'Select' button and a 'Send to users' field with a 'Select' button. The 'Add' button is highlighted in blue.



The screenshot shows the Zabbix web interface for managing Discovery rules. On the left is a dark blue sidebar with the Zabbix logo and navigation menu items: Dashboards, Monitoring, Services, Inventory, Reports, Data collection, and Template groups. The main content area is titled "Discovery rules" and shows a breadcrumb path: "All hosts / Zabbix server AGENT 2". The status is "Enabled" and the active tab is "ZBX". Other tabs include "SNMP", "IPMI", and "JMX". Summary statistics are shown: "Items 5", "Triggers 3", "Graphs", "Discovery rules 1", and "Web scenarios".

<input type="checkbox"/>	Host	Name ▲	Items	Triggers	Graphs	Hosts
<input type="checkbox"/>	Zabbix server AGENT 2	DiscoveryRule1	Item prototypes	Trigger prototypes	Graph prototypes	Host prototypes

0 selected

Script execution (non-configuration)

The screenshot shows the Zabbix web interface. On the left is a dark blue sidebar with the ZABBIX logo and navigation menu items: Dashboards, Monitoring (expanded), Problems, Hosts (selected), Latest data, Maps, Discovery, Services, Inventory, Reports, and Data collection. The main content area is titled 'Hosts' and has a dropdown menu open. The menu is divided into three sections: VIEW (Dashboards, Problems, Latest data, Graphs, Web, Inventory), CONFIGURATION (Host, Items, Triggers, Graphs, Discovery, Web), and SCRIPTS (Detect operating system, Ping, Traceroute). The 'Traceroute' script is currently selected. Below the menu, there are several input fields and a 'Select' button. At the bottom, a table displays monitoring data for two hosts.

Name ▲	Interface	Availability
Zabbix serv	127.0.0.1:10050	ZBX
Zabbix serv	127.0.0.1:10050	ZBX

Tasks reload (non-configuration)

reloading passive proxy config data (ZBXNEXT-1580), added in 6.2

The screenshot shows the ZABBIX web interface. On the left is a navigation sidebar with categories like Dashboards, Monitoring, Services, Inventory, Reports, Data collection, Alerts, Users, and Administration. The main content area is titled "Proxies" and contains a table with columns "Name" and "Mode". One proxy named "ALPHA2" is listed with a "Passive" mode. Below the table, it says "0 selected" and has a "Refresh configuration" button. A modal window titled "Proxy" is open, displaying a green success message: "Request created successfully". The modal has tabs for "Proxy", "Encryption", and "Timeouts". The "Proxy" tab is active, showing fields for "Proxy name" (ALPHA2), "Proxy mode" (Active/Passive), "Interface" (Address: 127.0.0.1, Port: 10051), and a "Description" text area. At the bottom of the modal are buttons for "Update", "Refresh configuration", "Clone", "Delete", and "Cancel".

Other non-configuration...

HA node status changes (ZBXNEXT-6923), added in 6.0

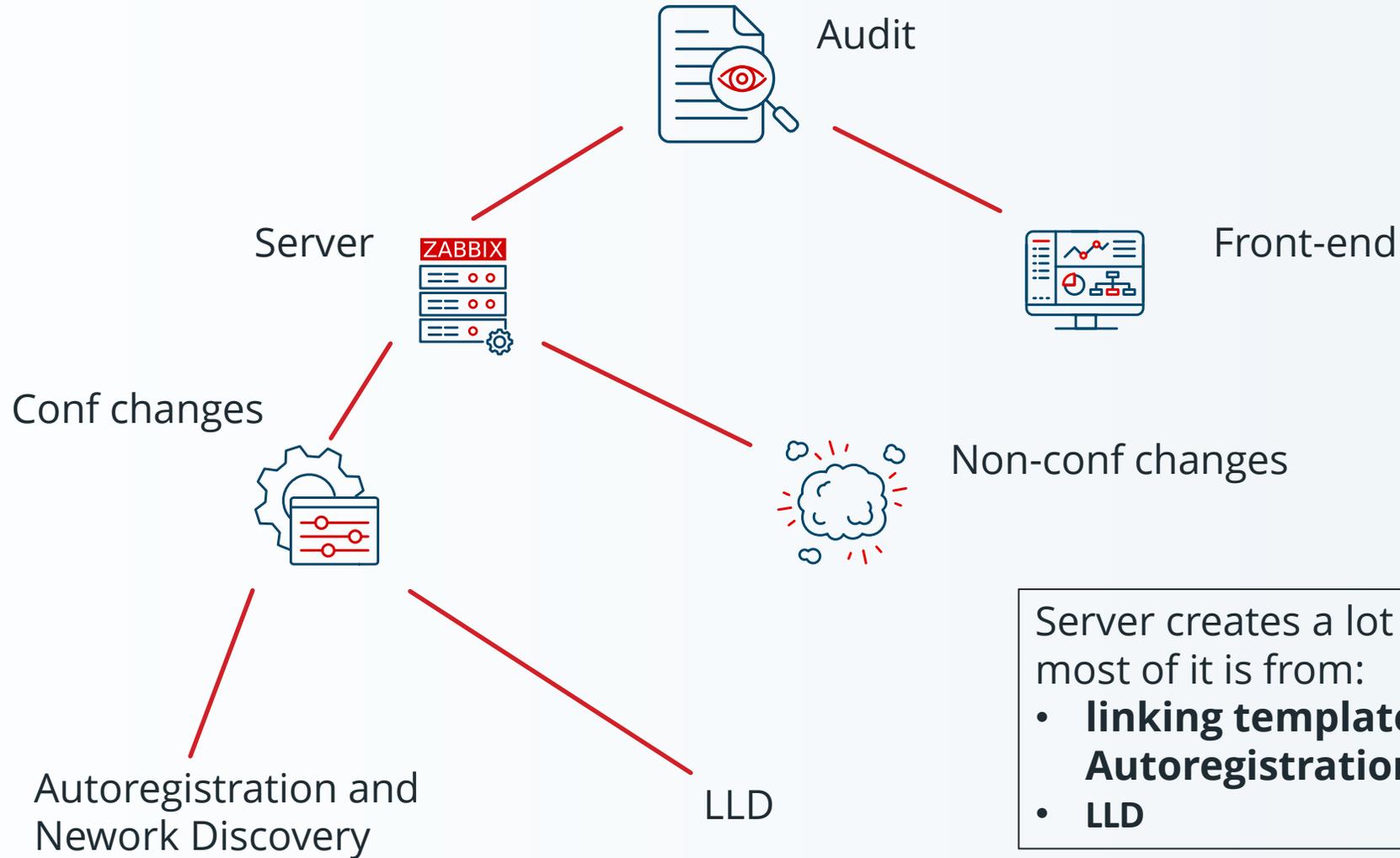
History push API request, sending data to Zabbix server via API (ZBXNEXT-8541), added in 7.0

The screenshot shows the Zabbix web interface's 'Audit log' page. On the left is a dark sidebar with navigation options: Dashboards, Monitoring, Services, Inventory, and Reports. The Reports section is expanded, showing options like System information, Scheduled reports, Availability report, Top 100 triggers, Audit log (which is selected), Action log, and Notifications. The main content area is titled 'Audit log' and features a search bar, a 'Zoom out' button, a 'Last 3 hours' time filter, and a 'Filter' button. Below these controls is a table with the following columns: Time, User, IP, Resource, ID, Action, Recordset ID, and Details. Three log entries are visible:

Time	User	IP	Resource	ID	Action	Recordset ID	Details
2024-04-23 04:14:18 PM	Admin	192.168.64.1	Proxy	1	Configuration refresh	clvceqtp0000nsiyym0mwadk	Description: ALPHA2
2024-04-23 04:14:08 PM	Admin	192.168.64.1	Script	10633	Execute	clvceqlhi00013diykw15gcrn	Description: Zabbix server AGENT 2 Details script.command: /usr/bin/traceroute 127.0.0.1 script.execute_on: 2
2024-04-23 04:13:52 PM	System		High availability node	0	Update	clvceq9tc000210iy3fphrlbv	hanode.status: 1 => 3

At the bottom right of the table area, it says 'Displaying 3 of 3 found'.

New Audit Scope Summary



Server creates a lot of configuration changes, most of it is from:

- **linking templates** during **Autoregistration** and **Network Discovery**
- **LLD**

New Audit Server Scope Summary

Most Zabbix server audit logic is in:

a) Linking of templates (as a result of **Autoregistration** or **Network Discovery**) with updates to:

- Hosts
- Items
- Triggers
- Graphs
- Discovery Rules (and prototypes of everything above)
- Web Scenarios

2) LLD, with the following entities created from prototypes:

- Hosts
- Items
- Triggers
- Graphs

New Audit Goals

- Simple to manage and fast.
- All Audit is stored in single table (Simpler and faster SQL queries).
- Bulk SQL inserts and efficient ids generation.

- Audit of particular entity stays longer than this entity. If entity - (host or user) is deleted – audit for it stays. Audit has independent housekeeping schedule.
- Can be disabled.

IDs for New Audit

Ids table:

```
zabbix=> select * from ids;
  table_name | field_name | nextid
-----+-----+-----
  actions   | actionid   |      7
  operations | operationid |     12
  optemplate | optemplateid |      3
  module    | moduleid   |     29
  profiles  | profileid  |     65
  housekeeper | housekeeperid |    1154
  hosts     | hostid     |   10632
  interface | interfaceid |      35
  hosts_groups | hostgroupid |     637
  hgset     | hgsetid    |      17
  hosts_templates | hosttemplateid |    460
  items     | itemid     |  47084
  triggers  | triggerid  |  23685
  functions | functionid  |  33628
(14 rows)
```

New audit could use ids table, but..

IDs for new Audit

CUID



Collision resistant id for horizontal scaling

clvc7m4ik0009e9iy2t4dpmja

c - lvc7m4ik - 0009 - e9iy - 2t4dpmja

timestamp - counter - client fingerprint - random string

New 'System' User

ZABBIX << ↻

- Dashboards
- Monitoring
- Services
- Inventory
- Reports
 - System information
 - Scheduled reports
 - Availability report
 - Top 100 triggers
 - Audit log

Audit log



Time	User	IP	Resource	ID	Action	Recordset ID	Details
2024-04-23 05:21:19 AM	Admin	192.168.64.1	User	1	Login	clvbrf2tm0000y5iyp1jacyvy	
2024-04-23 05:21:17 AM	Admin	192.168.64.1	User	1	Logout	clvbrf1h80000y3iybgmze1kk	
2024-04-23 05:20:14 AM	System		High availability node	0	Update	clvbrdoi70006q9iyy3yg0mrh	hanode.status: 3 => 1
2024-04-23 05:20:13 AM	System		Graph	2766	Add	clvbrdnt3000eqmiydmtvr454	Description: vda: Disk t graph: Added graph.flags: 4
2024-04-23 05:20:13 AM	System		Graph	2765	Add	clvbrdnt3000eqmiydmtvr454	Description: vda: Disk r graph: Added graph.flags: 4

UI Recordset ID



Time	User	IP	Resource	ID	Action	Recordset ID	Details
2024-04-23 05:21:19 AM	Admin	192.168.64.1	User	1	Login	clvbrf2tm0000y5iyp1jacyv	
2024-04-23 05:21:17 AM	Admin	192.168.64.1	User	1	Logout	clvbrf1h80000y3iybgmze1kk	
2024-04-23 05:20:14 AM	System		High availability node	0	Update	clvbrdoi70006q9iyy3yg0mrh	hanode.status: 3 => 1
2024-04-23 05:20:13 AM	System		Graph	2766	Add	clvbrdnt3000eqmiydmtr454	Description: vda: Disk t graph: Added graph.flags: 4
2024-04-23 05:20:13 AM	System		Graph	2765	Add	clvbrdnt3000eqmiydmtr454	Description: vda: Disk r graph: Added graph.flags: 4

Recordset ID

From the spec:

“To have the ability to recognize that some set of audit log records was created during the processing of separate operation, a new column "Recordset ID" for audit log records will be provided. Each audit log record of separate operation will have the same recordset ID. The recordset ID will be generated using CUID algorithm.”

- Script execution has one single recordset ID.
- During the linking - all newly created audit entries are saved with the same recordset ID.

Audit log

Time	User	IP
2024-04-23 05:21:19 AM	Admin	192.168.1.1
2024-04-23 05:21:17 AM	Admin	192.168.1.1
2024-04-23 05:20:14 AM	System	
2024-04-23 05:20:13 AM	System	

Details

```
item.description: The rate of total write time counter; used in `w_await` calculation.  
item.flags: 4  
item.history: 7d  
item.hostid: 10628  
item.itemid: 47157  
item.key: vfs.dev.write.time.rate[vda]  
item.master_itemid: 47151  
item.name: vda: Disk write time (rate)  
item.preprocessing[99438]: Added  
item.preprocessing[99438].params: $[7]
```

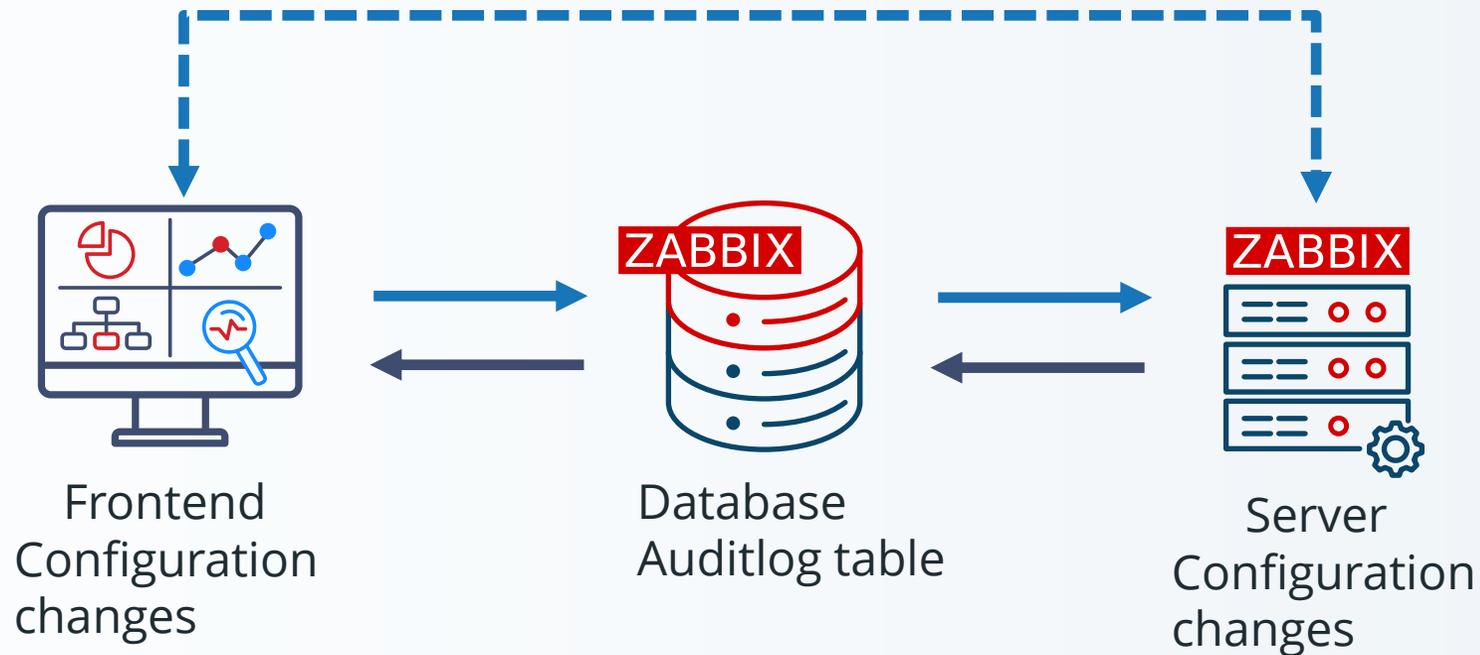
Ok

Graph 2766 Add clvbrdnt3000eqmiydmtr454 Description: vda: Disk utilization and queue

graph: Added
graph.flags: 4

Technical Implementation

Server audit has independent implementation from front-end, but they produce the same entries for same operations.



Technical Implementation

Database changes



Old auditlog and auditlog_details tables are removed during upgrade patch to 6.0.

New auditlog table is created.

Schema update

```
TABLE|auditlog|auditid|0
FIELD|auditid|t_id|NOT NULL|0
FIELD|userid|t_id|NOT NULL|0
FIELD|clock|t_time|'0'|NOT NULL|0
FIELD|action|t_integer|'0'|NOT NULL|0
FIELD|resourcetype|t_integer|'0'|NOT NULL|0
FIELD|note|t_varchar(128)|'|NOT NULL|0
FIELD|ip|t_varchar(39)|'|NOT NULL|0
FIELD|resourceid|t_id|NULL|0
FIELD|resourcename|t_varchar(255)|'|NOT NULL|0
INDEX|1|userid,clock
INDEX|2|clock
INDEX|3|resourcetype,resourceid
```

```
TABLE|auditlog|auditid|0
FIELD|auditid|t_cuid|NOT NULL|0
FIELD|userid|t_id|NULL|0
FIELD|username|t_varchar(100)|'|NOT NULL|0
FIELD|clock|t_time|'0'|NOT NULL|0
FIELD|ip|t_varchar(39)|'|NOT NULL|0
FIELD|action|t_integer|'0'|NOT NULL|0
FIELD|resourcetype|t_integer|'0'|NOT NULL|0
FIELD|resourceid|t_id|NULL|0
FIELD|resource_cuid|t_cuid|NULL|0
FIELD|resourcename|t_varchar(255)|'|NOT NULL|0
FIELD|recordsetid|t_cuid|NOT NULL|0
FIELD|details|t_longtext|'|NOT NULL|0
INDEX|1|userid,clock
INDEX|2|clock
INDEX|3|resourcetype,resourceid
```

- auditid is now CUID
- userid can be NULL (no more foreign reference on users table)
- username is added
- resource_cuid is added(alternative to resource, only for HA)
- recordsetid is added
- note and other auditlog_details table data now is in details (JSON)

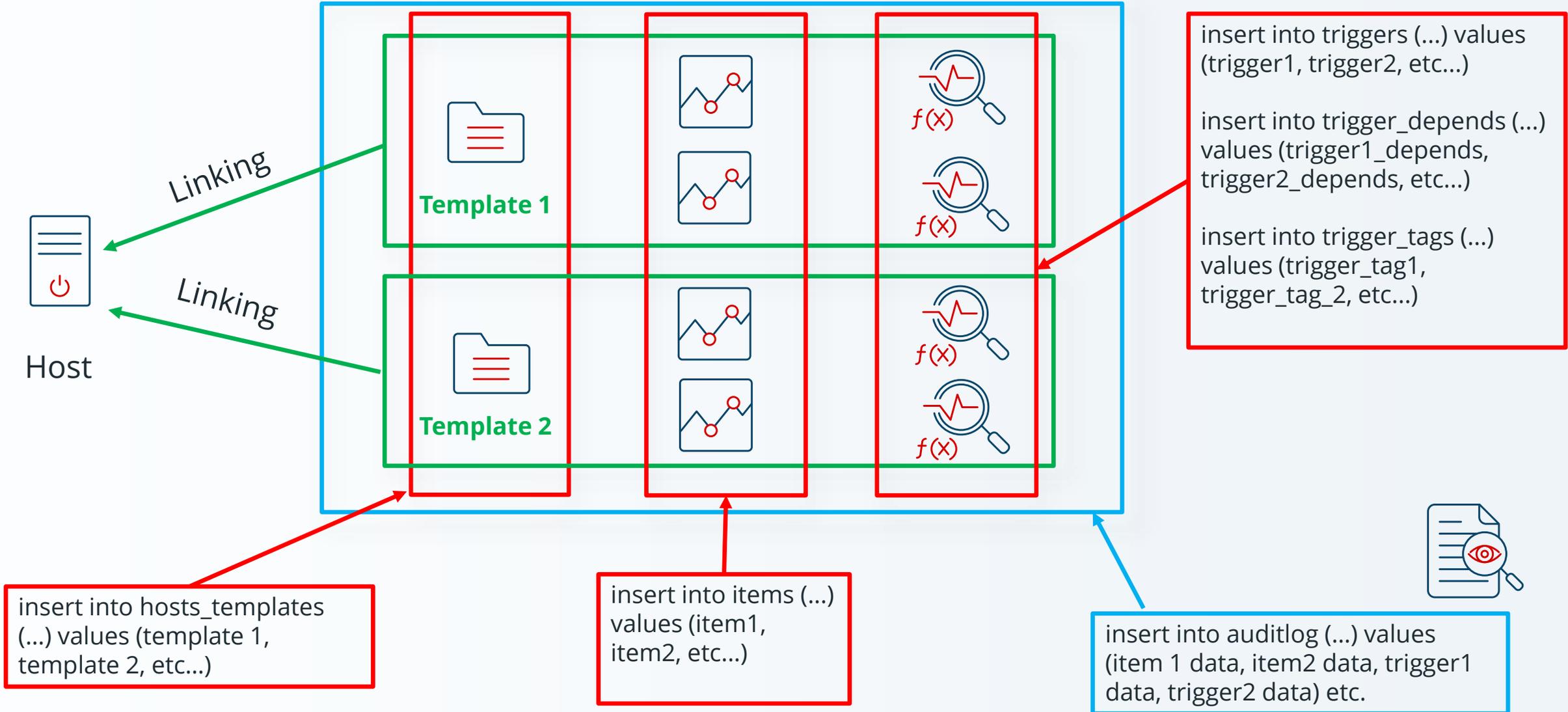
Technical Implementation

```
TABLE|auditlog|auditid|0
FIELD|auditid|t_id|NOT NULL|0
FIELD|userid|t_id|NOT NULL|0
FIELD|clock|t_time|'0'|NOT NULL|0
FIELD|action|t_integer|'0'|NOT NULL|0
FIELD|resourcetype|t_integer|'0'|NOT NULL|0
FIELD|note|t_varchar(128)|'|NOT NULL|0
FIELD|ip|t_varchar(39)|'|NOT NULL|0
FIELD|resourceid|t_id|NULL|0
FIELD|resourcename|t_varchar(255)|'|NOT NULL|0
INDEX|1|userid,clock
INDEX|2|clock
INDEX|3|resourcetype,resourceid
```

```
TABLE|auditlog|auditid|0
FIELD|auditid|t_cuid|NOT NULL|0
FIELD|userid|t_id|NULL|0
FIELD|username|t_varchar(100)|'|NOT NULL|0
FIELD|clock|t_time|'0'|NOT NULL|0
FIELD|ip|t_varchar(39)|'|NOT NULL|0
FIELD|action|t_integer|'0'|NOT NULL|0
FIELD|resourcetype|t_integer|'0'|NOT NULL|0
FIELD|resourceid|t_id|NULL|0
FIELD|resource_cuid|t_cuid|NULL|0
FIELD|resourcename|t_varchar(255)|'|NOT NULL|0
FIELD|recordsetid|t_cuid|NOT NULL|0
FIELD|details|t_longtext|'|NOT NULL|0
INDEX|1|userid,clock
INDEX|2|clock
INDEX|3|resourcetype,resourceid
```

Why there is no index on RecordSet ID ?

Bulk SQL



Performance impact



~4-5%

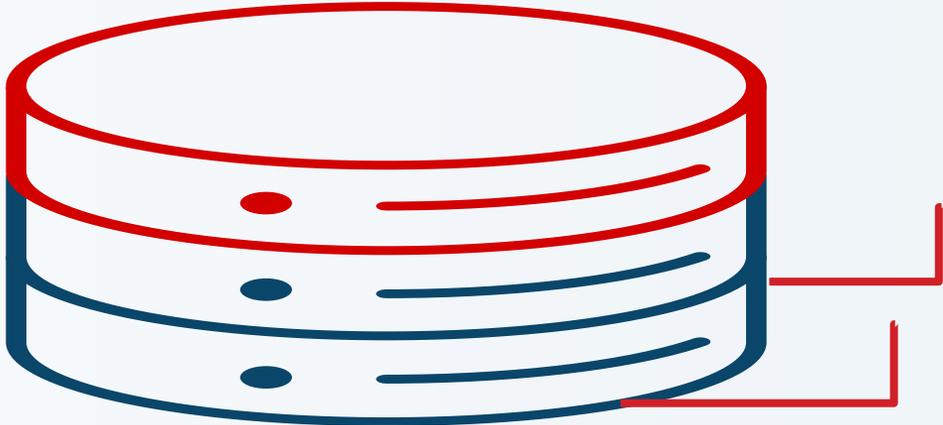
LINKING with audit	
MASTER	
1 000 triggers	00:00:0.19900000000052387
5 000 triggers	00:00:0.39099999999959837
10 000 triggers	00:00:1.743000000002212
20 000 triggers	00:00:3.754000000000815
40 000 triggers	00:00:7.335999999995693
68 000 triggers	00:00:12.494000000006054

LINKING without audit	
MASTER	
1 000 triggers	00:00:0.213999999999418
5 000 triggers	00:00:0.908000000003085
10 000 triggers	00:00:1.7699999999967986
20 000 triggers	00:00:3.518000000003667
40 000 triggers	00:00:7.49599999999185
68 000 triggers	00:00:11.953999999997905

Data storage impact

Impact on data storage requirements... (if forgotten about)

table_name	pg_size_pretty	pg_relation_size
auditlog	635 GB	681780338688
item_discovery	26 GB	28250169344



TimescaleDB

- Audit looks like a time-series data.
- Auditlog table has clocks column.
- Audit records are saved once and then only are read, never modified (and deleted).
- Can it be turned it into a hypertable ?
- Automated partitioning by time.
- + compression (Community edition license).



table, dimension
↓ ↓

```
SELECT create_hypertable('history', 'clock', chunk_time_interval => 86400, migrate_data => true);  
SELECT create_hypertable('history_uint', 'clock', chunk_time_interval => 86400, migrate_data => true);  
SELECT create_hypertable('history_log', 'clock', chunk_time_interval => 86400, migrate_data => true);  
SELECT create_hypertable('history_text', 'clock', chunk_time_interval => 86400, migrate_data => true);  
SELECT create_hypertable('history_str', 'clock', chunk_time_interval => 86400, migrate_data => true);  
SELECT create_hypertable('trends', 'clock', chunk_time_interval => 2592000, migrate_data => true);  
SELECT create_hypertable('trends_uint', 'clock', chunk_time_interval => 2592000, migrate_data => true);
```

So, why not just add:

```
SELECT create_hypertable('auditlog', 'clock', chunk_time_interval => 86400, migrate_data => true) ?
```

ERROR: cannot create a unique index without the column "clock" (used in partitioning ..

History uint indexes:

"history_uint_pkey" PRIMARY KEY, btree (itemid, **clock**, ns)

Auditlog Indexes:

"auditlog_pkey" PRIMARY KEY, btree (auditid)

"auditlog_1" btree (userid, clock)

"auditlog_2" btree (clock)

"auditlog_3" btree (resourcetype, resourceid)

Primary key has no clock...

TimescaleDB

Every unique index needs to contain clock dimension against which we partition by.
In Auditlog Primary key has no clock, but it not a regular ID...

It is **CUID**:

clvb1wfub00027viy6mphm75s



Timestamp

So, we can extract it and use for partitioning by time.

```
DROP FUNCTION IF EXISTS cuid_timestamp(cuid varchar(25));
CREATE OR REPLACE FUNCTION cuid_timestamp(cuid varchar(25)) RETURNS
integer AS $$
BEGIN
    RETURN CAST(base36_decode(substring(cuid FROM 2 FOR 8))/1000 AS
integer);
END;
$$ LANGUAGE 'plpgsql' IMMUTABLE;

PERFORM create_hypertable('auditlog', 'auditid', chunk_time_interval => 604800,
    time_partitioning_func => 'cuid_timestamp', migrate_data => true, if_not_exists
=> true);
```

ZBXNEXT-8520, added in 7.0

May take some time migrate existing data..

Administration

ZABBIX << ↻

 Dashboards

 Monitoring ▾

 Services ▾

 Inventory ▾

Audit log

Enable audit logging

Log system actions 

Enable internal housekeeping

* Data storage period

Administration

Enable audit logging

The screenshot shows the Zabbix Administration interface. On the left is a dark blue sidebar with the ZABBIX logo and navigation links for Dashboards, Monitoring, Services, and Inventory. The main content area is titled "Audit log" and contains several settings:

- Enable audit logging**: A checkbox that is checked, highlighted with a red rectangular box.
- Log system actions**: A checkbox that is checked, with a help icon (question mark) to its left.
- Enable internal housekeeping**: A checkbox that is checked.
- * Data storage period**: A text input field containing "31d".

At the bottom of the settings area are two buttons: "Update" and "Reset defaults".

Disables ALL audit – including front-end.

Log system actions (7.0)

The screenshot shows the Zabbix Administration interface. On the left is a dark blue sidebar with the ZABBIX logo and navigation links: Dashboards, Monitoring, Services, and Inventory. The main content area is titled "Audit log" and contains several settings:

- Enable audit logging
- Log system actions (highlighted with a red box)
- Enable internal housekeeping
- * Data storage period:

At the bottom of the settings area are two buttons: "Update" and "Reset defaults".

Disables audit done by Zabbix server during Autoregistration, Network Discovery and LLD.

Audit has its own Housekeeping Schedule

The screenshot shows the ZABBIX administration interface. On the left is a dark blue sidebar with the ZABBIX logo and navigation links for Dashboards, Monitoring, Services, and Inventory. The main content area is titled 'Audit log' and contains several configuration options:

- Enable audit logging
- Log system actions
- Enable internal housekeeping (highlighted with a red box)
- * Data storage period (highlighted with a red box)

At the bottom of the configuration area are two buttons: 'Update' and 'Reset defaults'.

If user, host, trigger, graph is deleted (including housekeeper) - all audit related to it stays.

The ZABBIX logo consists of the word "ZABBIX" in a bold, white, sans-serif font, centered within a solid red rectangular box. The background of the entire slide is a dark blue gradient with a faint, glowing network of white lines and nodes, and a semi-transparent world map in the center-right.

ZABBIX

Artjoms Rimdjonoks

C Developer