



ZABBIX
PREMIUM PARTNER

ZABBIX
CERTIFIED TRAINER

Webinar

What's new in Zabbix 7.4

all your microphones are muted

ask your questions in Q&A, not in the Chat

use Chat for discussion, networking or applause

Main Focus

Zabbix 7.4 brings some long expected features, improves security and adds few nice surprises

- ▶ Nested low-level discovery
- ▶ Host prototypes on discovered hosts
- ▶ OAuth 2.0 authentication for email media
- ▶ Security (Encryption between frontend and server, Resolving secret vault macros by server/proxy independently)
- ▶ Notifications (Separate menu section for user notifications, Managing own user media)
- ▶ Host Wizard, improvements in widgets & maps, new functions, macros & more

1

Host Wizard



Host Wizard

- ▶ The host wizard guides Zabbix users through initial host creation and configuration steps.

×

Welcome to the Host Wizard

The Host Wizard will help you set up your monitoring target (device, application, service, etc.) in Zabbix.

You can always access Host Wizard from Data collection > Hosts.

☐ Do not show welcome screen

Cancel

Next

Host Wizard

- ▶ Only a single template can be added per the Host Wizard session.
- ▶ More templates can be added by opening the Host Wizard and selecting an existing host.


×

Select a template:

Linux by Zabbix agent

Create or select a host

A few more steps




Some templates (332) are incompatible with the Host Wizard. See [how to update them](#). Custom templates are not supported.


Select a template

A template is a set of predefined configurations (metrics to be collected, conditions for generating alerts, etc.) designed for your monitoring target.

Linux

Type a keyword to search for templates.

Data collection 

Agent mode 

AllAgent-basedAgentless

AllActivePassive

[Cancel](#)

[Back](#)

[Next](#)

Host Wizard

- ▶ Here you can define a new host or select an existing one. In case you select an existing host, the template settings chosen in the previous step will be applied.

×

Select a template:
Linux by Zabbix agent

Create or select a host:
initMAX (new)

A few more steps

Create or select a host

The template you selected (Linux by Zabbix agent) must be linked to a host - an entity in Zabbix that represents your monitoring target.

Hosts are organized into host groups for easier management and access control.

* Host name

initMAX (new) ×

Select

Start typing or click Select to choose an existing host, or enter a new host name.

* Host groups

initMAX (new) ×

Select

type here to search

Start typing or click Select to choose existing host groups, or enter a new host group name.

[Cancel](#)

Back

Next

Host Wizard

- Here you must configure connection options for your host in several steps. The required settings depend on the selected item types and their connection methods, including SNMP.

×

Select a template:
Linux by Zabbix agent

Create or select a host:
initMAX (new)

Install Zabbix agent

Add host interface

Configure host

Install Zabbix agent

The template you selected (Linux by Zabbix agent) requires Zabbix agent to be installed and running on your monitoring target.

Skip OS selection if you already have Zabbix agent installed.

1. Verify Zabbix server, proxy, or cluster address

Enter the IP/DNS address and port of your Zabbix server, proxy, or cluster configuration.

Example:
192.0.2.0:10051, [2001:db8::]:10051, zbx1.local:10051;zbx2.local:10051

Zabbix agent must be able to connect to the specified address or list of addresses.

Use:

- Colon to separate IP/DNS address from port
- Comma to separate multiple Zabbix servers, proxies, or clusters
- Semicolon to separate clusters (one or more server addresses)

[Cancel](#)

BackNext

Host Wizard

- ▶ Only for Zabbix agent connections, the wizard assists you with PSK configuration for new hosts. This setting is enforced initially but can be disabled later directly on the host.

×

Select a template:
Linux by Zabbix agent

Create or select a host:
initMAX (new)

Install Zabbix agent

Add host interface

Configure host

2. Configure encryption

Communication between Zabbix agent and server/proxy is secured with the pre-shared key (PSK) encryption method.

* Pre-shared key identity

initMAX

Enter a non-secret pre-shared key identity string. Avoid including sensitive data.

* Pre-shared key

95dee422a17be034f9d2132961a586295c72a3ee1169c2bda32a2e849c380664

Generate new

Generate a secret pre-shared key hexadecimal string.

3. Select the OS of your monitoring target

[Cancel](#)

BackNext

Host Wizard

- ▶ The wizard also assists you with installing the Zabbix agent on various platforms if required. You can skip this step or remove the PSK section here if you plan to disable it later.

×

Select a template:
Linux by Zabbix agent

Create or select a host:
initMAX (new)

Install Zabbix agent

Add host interface

Configure host

Generate a secret pre-shared key hexadecimal string.

3. Select the OS of your monitoring target

Linux☒

Windows☐

Other☐

4. Set up Zabbix agent on your monitoring target by executing the following script [bash under root]:

```
$(command -v curl || echo $(command -v wget) -O -)  
https://cdn.zabbix.com/scripts/7.4/install-zabbix.sh | bash -s --  
--server-host '127.0.0.1' --hostname 'initMAX' --psk-identity-  
stdin --psk  
95dee422a17be034f9d2132961a586295c72a3ee1169c2bda32a2e849c380664
```

[Cancel](#)

BackNext

Host Wizard

- ▶ Here you must fill in your host interface address. You can also see a helpful explanation about why this is required.

×

Select a template:
Linux by Zabbix agent

Create or select a host:
initMAX (new)

Install Zabbix agent

Add host interface

Configure host

Add host interface

The template you selected (Linux by Zabbix agent) requires the Agent interface to be added to the host (initMAX).

Note: Agent must be configured and enabled on your monitoring target.

* Agent address
127.0.0.1

* Agent port
10050

Enter the IP/DNS address and port of the Zabbix agent installed on your monitoring target.

[Cancel](#)

BackNext

Host Wizard

- ▶ If the template contains additional important information, you will see it listed here.
- ▶ Here you'll see a brief explanation of selected macros and thresholds.

×

Select a template:
Linux by Zabbix agent

Create or select a host:
initMAX (new)

Install Zabbix agent

Add host interface

Configure host

Configure host (1/2)

The template you selected (Linux by Zabbix agent) requires additional configuration.

Overview

This is an official Linux template. It requires Zabbix agent 7.4 or newer.

Notes on filesystem (FS) discovery:

- The ext4/3/2 FS reserves space for privileged usage, typically set at 5% by default.
- BTRFS allocates a default of 10% of the volume for its own needs.
- To mitigate potential disasters, FS usage triggers are based on the maximum available space.
 - Utilization formula: $\text{pused} = 100 - 100 * (\text{available} / \text{total} - \text{free} + \text{available})$
- The FS utilization chart, derived from graph prototypes, reflects FS reserved space as the difference between used and available space from the total volume.

[Cancel](#)

BackNext

Host Wizard

- ▶ On this page, you'll see basic parameters adjustable via macros, along with their default values.
- ▶ Parameters are divided into several categories such as Thresholds and Filters, and you can use both text fields and selection buttons.

×

Select a template:
Linux by Zabbix agent

Create or select a host:
initMAX (new)

Install Zabbix agent

Add host interface

Configure host

Configure host (2/2)

To complete the setup, configure the following variables (host macros).

Seconds since the last Zabbix agent seen

T ▾

☐ Interfaces control

Macro: {\$AGENT.TIMEOUT}

Timeout after which agent is considered unavailable.

Macro: {\$IFCONTROL}

Fire a trigger when the interface operational status changes to "Link down".

▾ Thresholds

Host Wizard

- ▶ On the last page, simply confirm your selected settings.
- ▶ The wizard helps avoid missed settings when adding new templates.

×

Select a template:
Linux by Zabbix agent

Create or select a host:
initMAX

Install Zabbix agent

Add host interface

Configure host

✓

Host added successfully

×

Configuration complete

Click Finish to navigate to the Latest data section and view the most recent data for your host (initMAX).

Finish

Host Wizard

- ▶ If you're upgrading from an earlier Zabbix version, templates must be upgraded to work with the Host Wizard. For instructions, see Template upgrade.

https://www.zabbix.com/documentation/current/en/manual/config/templates_out_of_the_box#template-upgrade

- ▶ The guidelines that have not been updated can be found in a separate section on the Zabbix documentation page.

<https://www.zabbix.com/documentation/guidelines/en/thosts>

Host Wizard

```
zabbix_export:
  version: '7.4'
  template_groups:
    - uuid: 846977d1dfed4968bc5f8bdb363285bc
      name: 'Templates/Operating systems'
  templates:
    - uuid: f8f7908280354f2abeed07dc788c3747
      template: 'Linux by Zabbix agent'
      name: 'Linux by Zabbix agent'
      description: |
        ...
      wizard_ready: 'YES'
      readme: |
        ## Overview
        This is an official Linux template. It requires Zabbix agent 7.4 or newer.
        ...
      vendor:
        name: Zabbix
        version: 7.4-2
      ...
```

Host Wizard

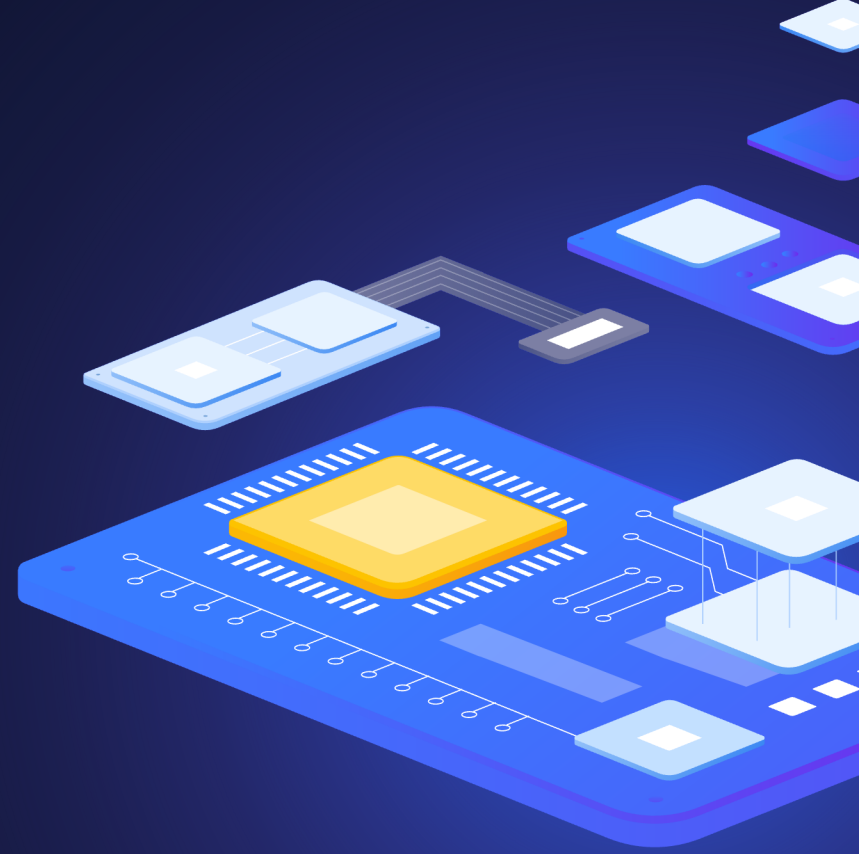
```
...
macros:
- macro: '{$AGENT.TIMEOUT}'
  value: 3m
  description: 'Timeout after which agent is considered unavailable...'
  config:
    type: TEXT
    priority: '1'
    label: 'Seconds since the last Zabbix agent seen'
    description: 'Timeout after which agent is considered unavailable.'
- macro: '{$CPU.UTIL.CRIT}'
  value: '90'
  description: 'Critical threshold of CPU utilization expressed in %.'
  config:
    type: TEXT
    priority: '2'
    section_name: Thresholds
    label: 'Threshold of CPU utilization expressed'
    description: 'Critical threshold of CPU utilization expressed in %.'
    regex: '^-[?]( [0-9]+|(( [0-9]+)\.([0-9]+)))$'
...
```

Host Wizard

```
...
- macro: '{$IFCONTROL}'
  value: '1'
  description: 'Link status trigger will be fired only for interfaces where the context...'
  config:
    type: CHECKBOX
    priority: '19'
    label: 'Interfaces control'
    description: 'Fire a trigger when the interface operational status changes...'
    options:
      - checked: '1'
        unchecked: '0'
...
```

2

Nested low-level discovery



Nested low-level discovery rules

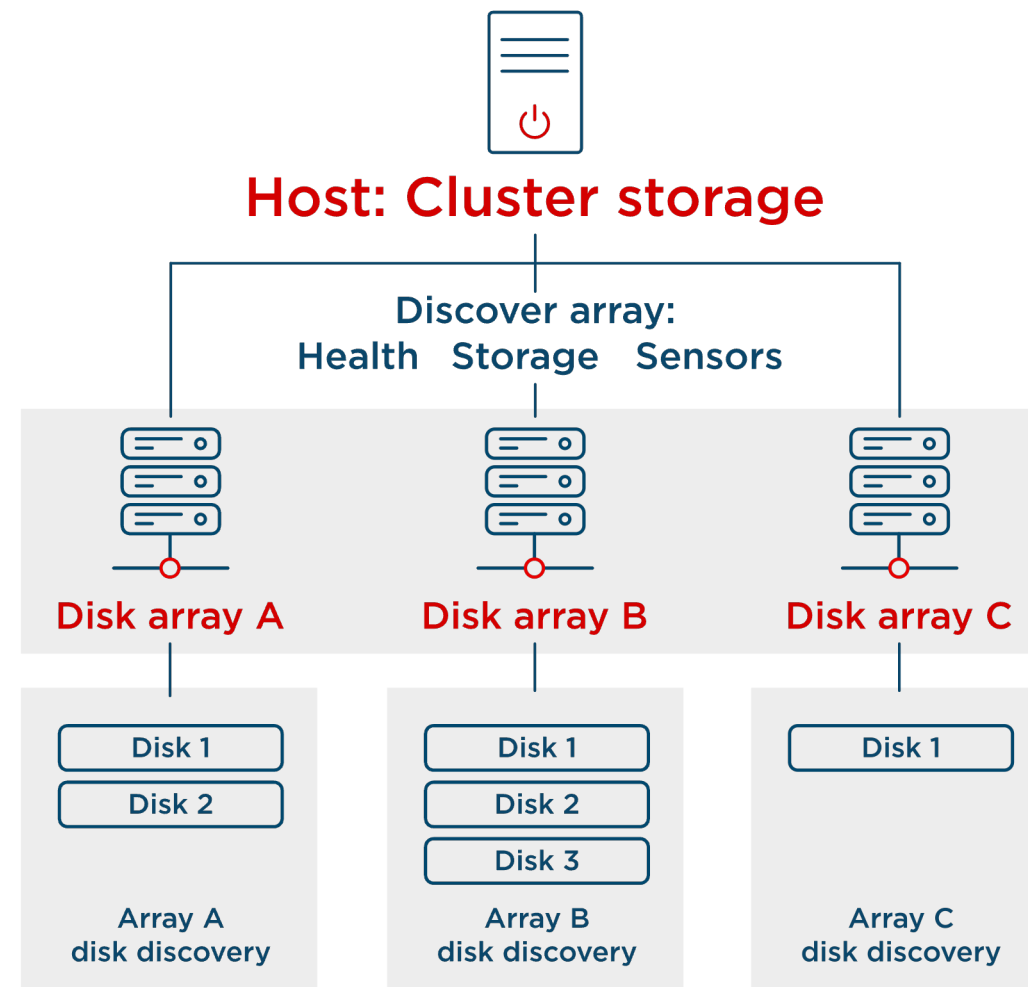
Zabbix 7.4 introduces the ability to create low-level discovery rule prototypes

- ▶ Each low-level discovery rule prototype can have its own item, trigger, graph, host and discovery prototypes
- ▶ This way multiple levels of discovery can be performed from a single multi-level JSON array
- ▶ Unlimited levels of nesting are supported

Nested low-level discovery rules

Nested low-level discovery can be used to:

- ▶ Discover database instances and use nested low-level discovery to discover instance tables
- ▶ Discover services or applications and use nested low-level discovery to discover the underlying components
- ▶ Discover hypervisors and use nested low-level discovery to discover virtual machines and containers



Nested low-level discovery rules

- ▶ New low-level discovery rule type - nested
- ▶ Can have it's own prototypes, including discovery prototypes

Discovery prototypes

All hosts / Database Cluster Enabled ZBX Discovery list / Discover databases and tablespaces Item prototypes 1 Trigger prototypes Graph prototypes Host prototypes Discovery prototypes 1

Discovery prototype Preprocessing 1 LLD macros 1 Filters Overrides

* Name Discover tablespaces for {#DB}

Type Nested

* Key db.tablespace.discovery[{#DB}]

* Delete lost resources ? Never Immediately After 7d

* Disable lost resources ? Never Immediately After

Discovery rules

All hosts / Database Cluster Enabled ZBX Items 12 Triggers Graphs Discovery rules 4 Web scenarios

Host groups type here to search Select Type All

Hosts Database Cluster x type here to search Select Update interval

Name

Key

Delete lost resources All Never Immediately After

Disable lost resources All Never Immediately After

State All Normal Not supported

Status All Enabled Disabled

Apply Reset

	Host	Name ▲	Items	Triggers	Graphs	Hosts	Discovery rules	Key	Interval	Type	Status	Info
<input type="checkbox"/>	Database Cluster	Discover databases and tablespaces	Item prototypes 1	Trigger prototypes	Graph prototypes	Host prototypes	Discovery prototypes 1	dbcluster.discovery		Zabbix trapper	Enabled	
<input type="checkbox"/>	Database Cluster	Discover databases and tablespaces: Discover tablespaces for db1	Item prototypes 1	Trigger prototypes	Graph prototypes	Host prototypes	Discovery prototypes	db.tablespace.discovery[db1]		Nested	Enabled	
<input type="checkbox"/>	Database Cluster	Discover databases and tablespaces: Discover tablespaces for db2	Item prototypes 1	Trigger prototypes	Graph prototypes	Host prototypes	Discovery prototypes	db.tablespace.discovery[db2]		Nested	Enabled	
<input type="checkbox"/>	Database Cluster	Discover databases and tablespaces: Discover tablespaces for db3	Item prototypes 1	Trigger prototypes	Graph prototypes	Host prototypes	Discovery prototypes	db.tablespace.discovery[db3]		Nested	Enabled	

Displaying 4 of 4 found

3

Nested host prototypes



Nested host prototypes

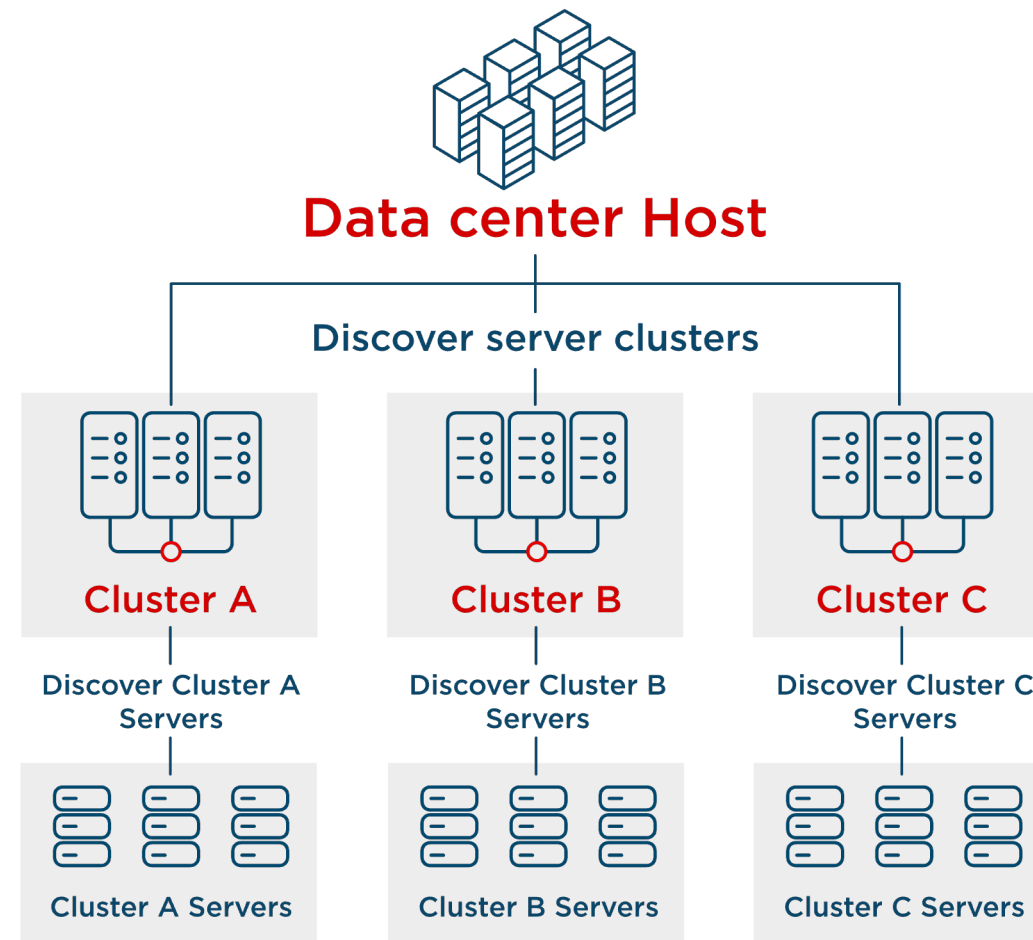
Hosts discovered from host prototypes can now use low-level discovery rules to create hosts of their own

- ▶ Nested host prototypes can be defined on as many levels as required
- ▶ Nested host prototypes can be used similarly to nested low-level discovery rules
- ▶ Nested host prototypes and low-level discovery rules enable a variety of new use cases for automated host and item detection workflows

Nested host prototypes

Nested host prototypes are useful when discovering multi-level entities:

- ▶ Discover server cluster hosts, which in turn discover individual cluster node hosts
- ▶ Discover database hosts, which in turn discover hosts for database tables
- ▶ Discover storage array hosts, which in turn discover storage devices per array
- ▶ Discover hypervisor hosts, which in turn discover virtual machine hosts



4

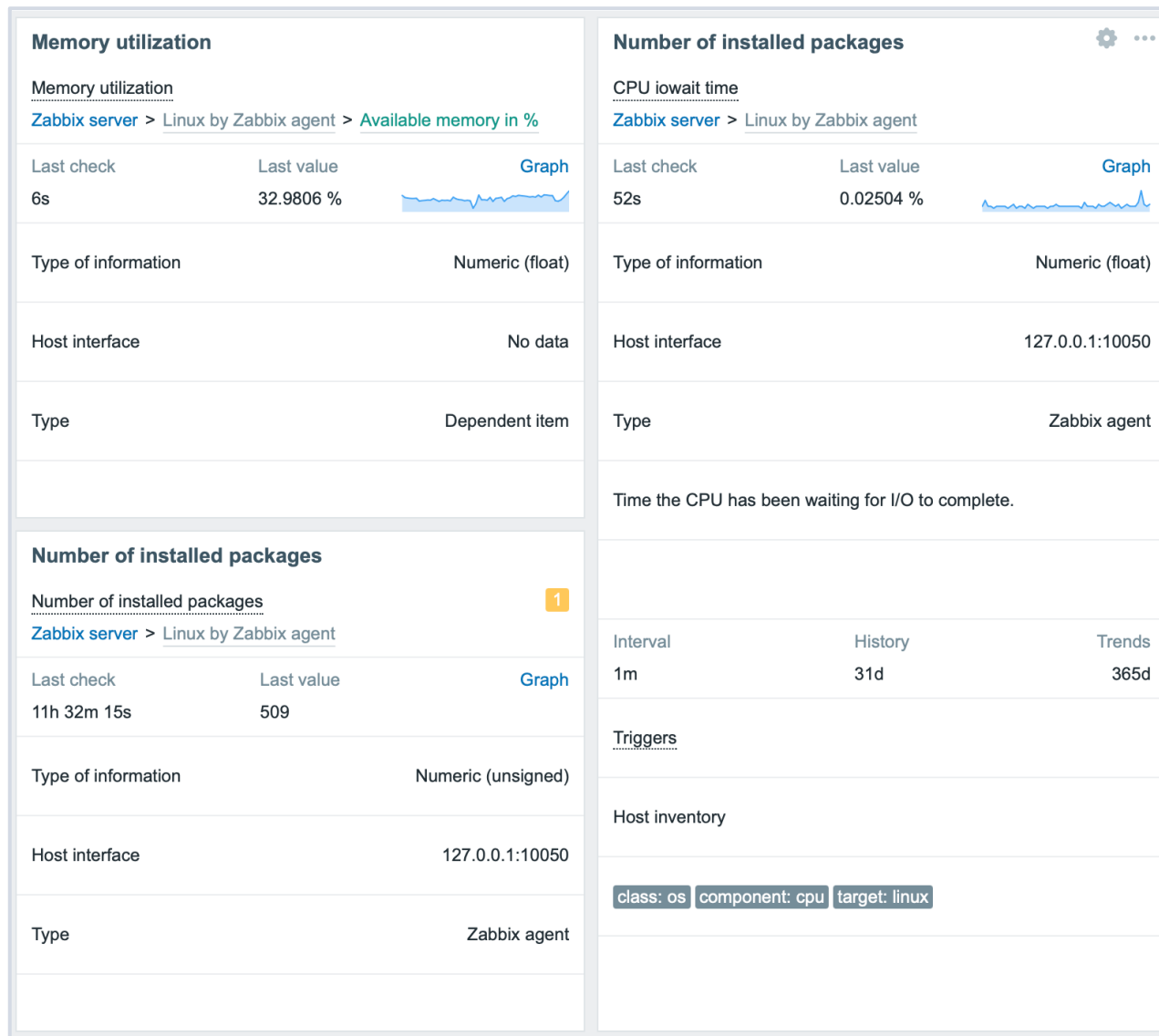
Item card widget



Item card widget

Item card widget provides a customizable view of an item and its various attributes


- ▶ Select from a list of fields to display
- ▶ Display the fields in any order



The screenshot displays two item card widgets side-by-side. The left widget is for 'Memory utilization' and the right is for 'Number of installed packages'. Both widgets show a table of attributes and a graph of the last check.


Memory utilization

Memory utilization
[Zabbix server](#) > [Linux by Zabbix agent](#) > [Available memory in %](#)

Last check	Last value	Graph
6s	32.9806 %	
Type of information	Numeric (float)	
Host interface	No data	
Type	Dependent item	


Number of installed packages

Number of installed packages
[Zabbix server](#) > [Linux by Zabbix agent](#)

Last check	Last value	Graph
11h 32m 15s	509	
Type of information	Numeric (unsigned)	
Host interface	127.0.0.1:10050	
Type	Zabbix agent	

Number of installed packages

Number of installed packages
[Zabbix server](#) > [Linux by Zabbix agent](#)

Last check	Last value	Graph
52s	0.02504 %	
Type of information	Numeric (float)	
Host interface	127.0.0.1:10050	
Type	Zabbix agent	

Time the CPU has been waiting for I/O to complete.

Interval	History	Trends
1m	31d	365d

Triggers

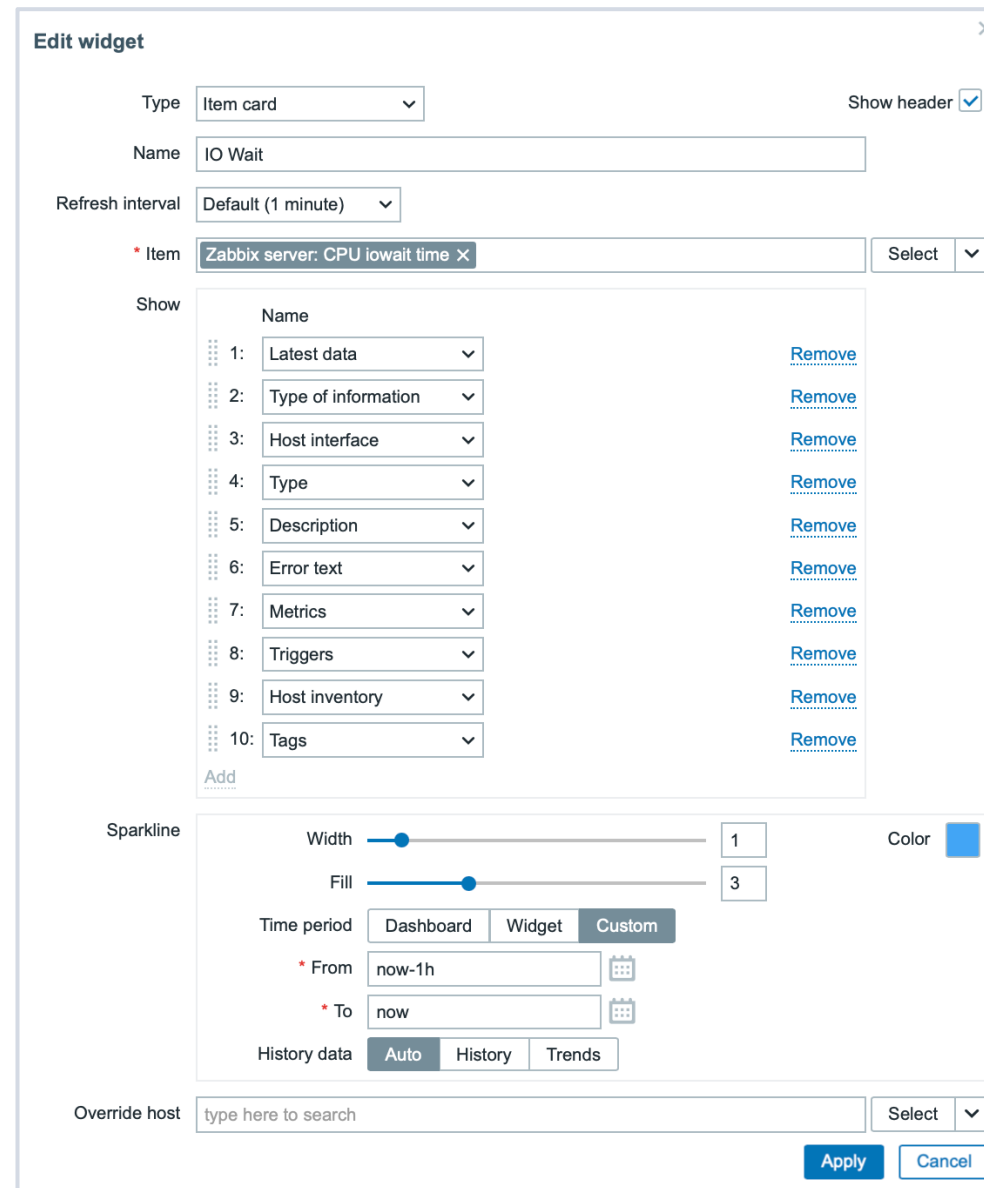
Host inventory

class: os component: cpu target: linux

Item card widget

The item card widget can display information like:

- › Latest data
- › Type of information
- › Host interface
- › Type
- › Description
- › Error text
- › Metrics
- › Triggers
- › Host inventory
- › Tags
- › Sparkline



The screenshot shows the 'Edit widget' configuration window for an 'Item card' widget. The configuration includes the following fields and options:

- Type:** Item card (dropdown)
- Show header:** ☒
- Name:** IO Wait (text input)
- Refresh interval:** Default (1 minute) (dropdown)
- Item:** Zabbix server: CPU iowait time (dropdown with a close button and a 'Select' dropdown)
- Show:** A list of 10 items to display, each with a dropdown menu and a 'Remove' link:
 - 1: Latest data
 - 2: Type of information
 - 3: Host interface
 - 4: Type
 - 5: Description
 - 6: Error text
 - 7: Metrics
 - 8: Triggers
 - 9: Host inventory
 - 10: Tags
- Sparkline:** A section for configuring a sparkline chart with sliders for Width (set to 1) and Fill (set to 3), a Color picker (blue), and a Time period selector (Dashboard, Widget, Custom). Below this are 'From' (now-1h) and 'To' (now) date pickers, and a History data selector (Auto, History, Trends).
- Override host:** A text input field with a 'Select' dropdown.
- Buttons:** Apply and Cancel at the bottom right.

5

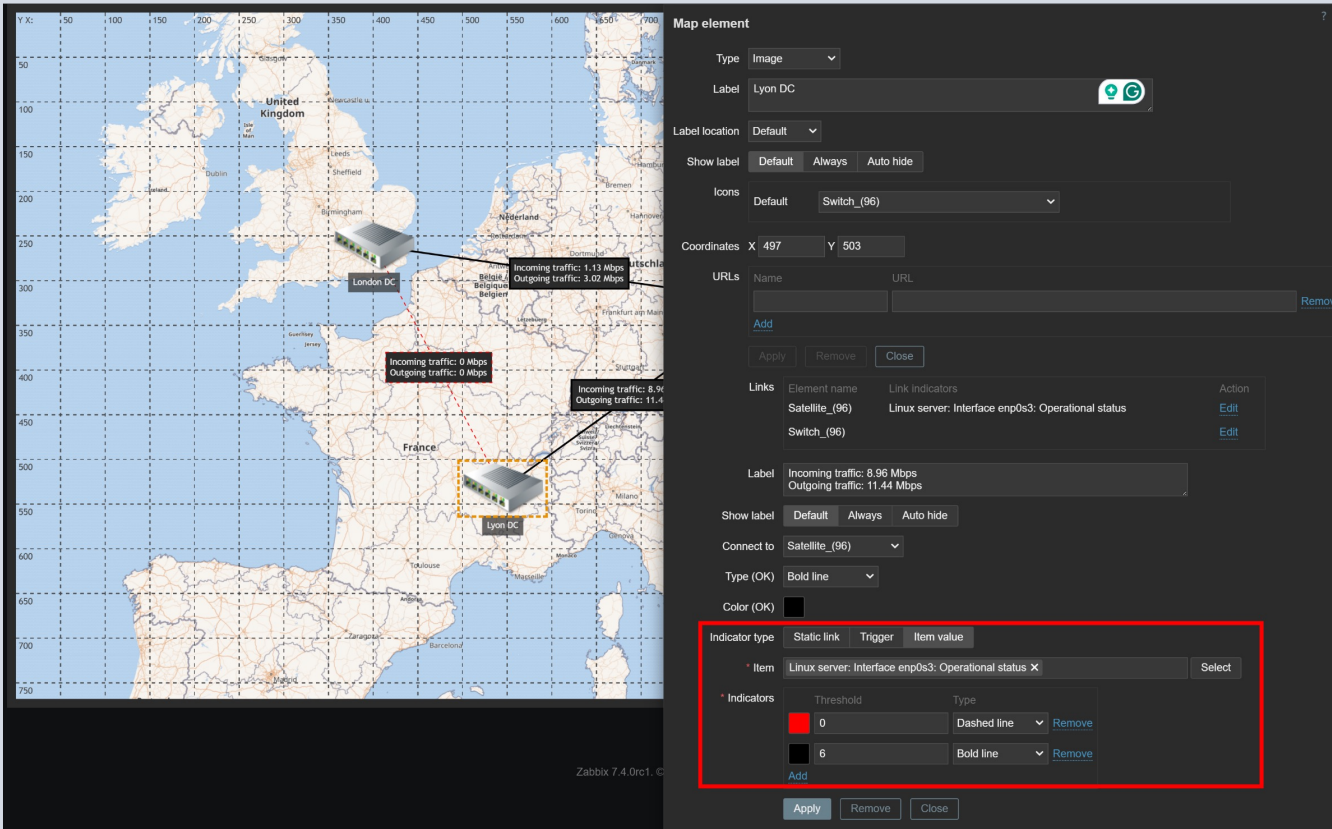
Network map improvements



Network map improvements

Various network map improvements have been introduced:

- ▶ Map background images can now be scaled proportionally to map dimensions
- ▶ Map links now support link indicators based on item value thresholds
- ▶ Map element icons can now be ordered when placed on top of one another



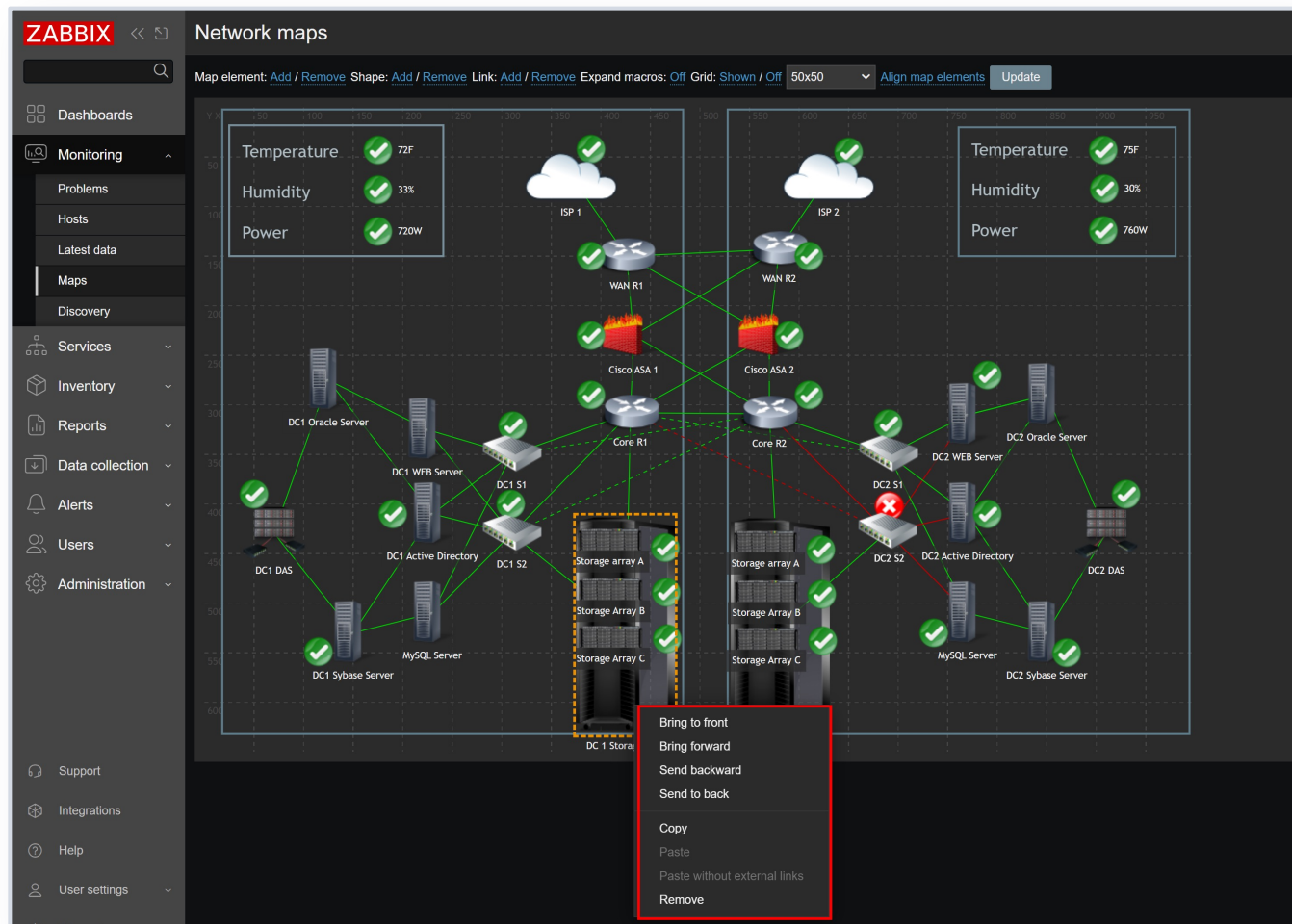
The screenshot displays the Zabbix 7.4 network map interface. On the left, a map of Europe shows several data centers (represented by server icons) and their connections. The map is overlaid with a grid. On the right, the 'Map element' configuration panel is visible. The panel includes fields for 'Type' (Image), 'Label' (Lyon DC), 'Label location' (Default), 'Show label' (Default, Always, Auto hide), 'Icons' (Default, Switch_(96)), and 'Coordinates' (X: 497, Y: 503). Below these are 'URLs' and 'Links' sections. The 'Links' section shows a table with columns for 'Element name', 'Link indicators', and 'Action'. The table contains two rows: 'Satellite_(96)' with 'Linux server: Interface enp0s3: Operational status' and 'Switch_(96)'. The 'Label' field for the selected link shows 'Incoming traffic: 8.96 Mbps' and 'Outgoing traffic: 11.44 Mbps'. The 'Show label' field is set to 'Default'. The 'Connect to' field is set to 'Satellite_(96)'. The 'Type (OK)' field is set to 'Bold line'. The 'Color (OK)' field is set to black. The 'Indicator type' section is highlighted with a red box and shows a table with columns for 'Item', 'Threshold', 'Type', and 'Remove'. The table contains two rows: 'Linux server: Interface enp0s3: Operational status' with a threshold of '0' and a type of 'Dashed line', and 'Linux server: Interface enp0s3: Operational status' with a threshold of '6' and a type of 'Bold line'.

Item	Threshold	Type	Remove
Linux server: Interface enp0s3: Operational status	0	Dashed line	Remove
Linux server: Interface enp0s3: Operational status	6	Bold line	Remove

Network map improvements

Various network map improvements have been introduced:

- ▶ Map element icons can now be ordered when placed on top of one another
- ▶ Host group map elements will now take into account nested host groups when displaying host group related information
- ▶ Map link and element labels can now be hidden and only be displayed on mouse hover



6

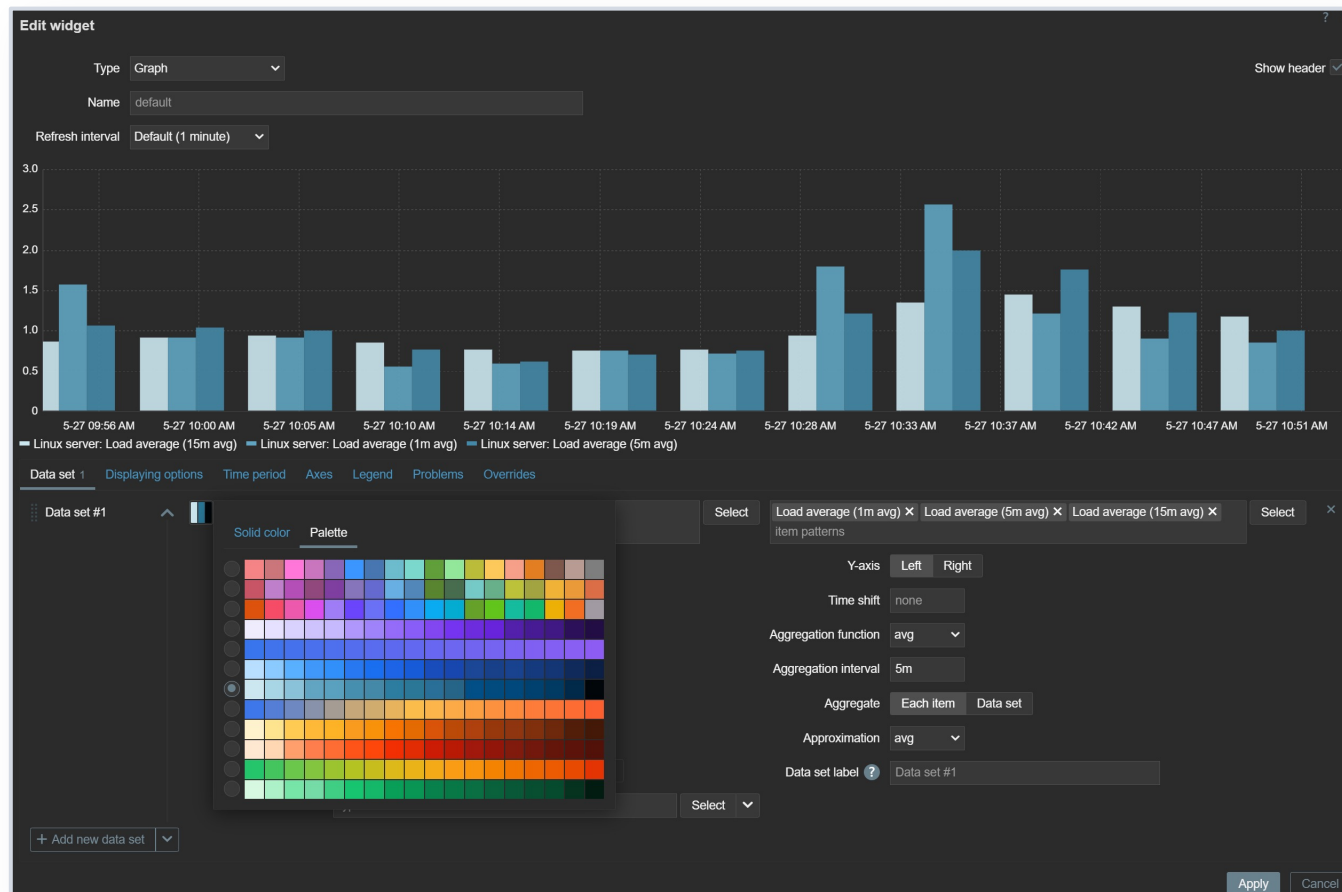
Dashboard improvements



Dashboard improvements

Various dashboard improvements to facilitate faster and smoother dashboard configuration

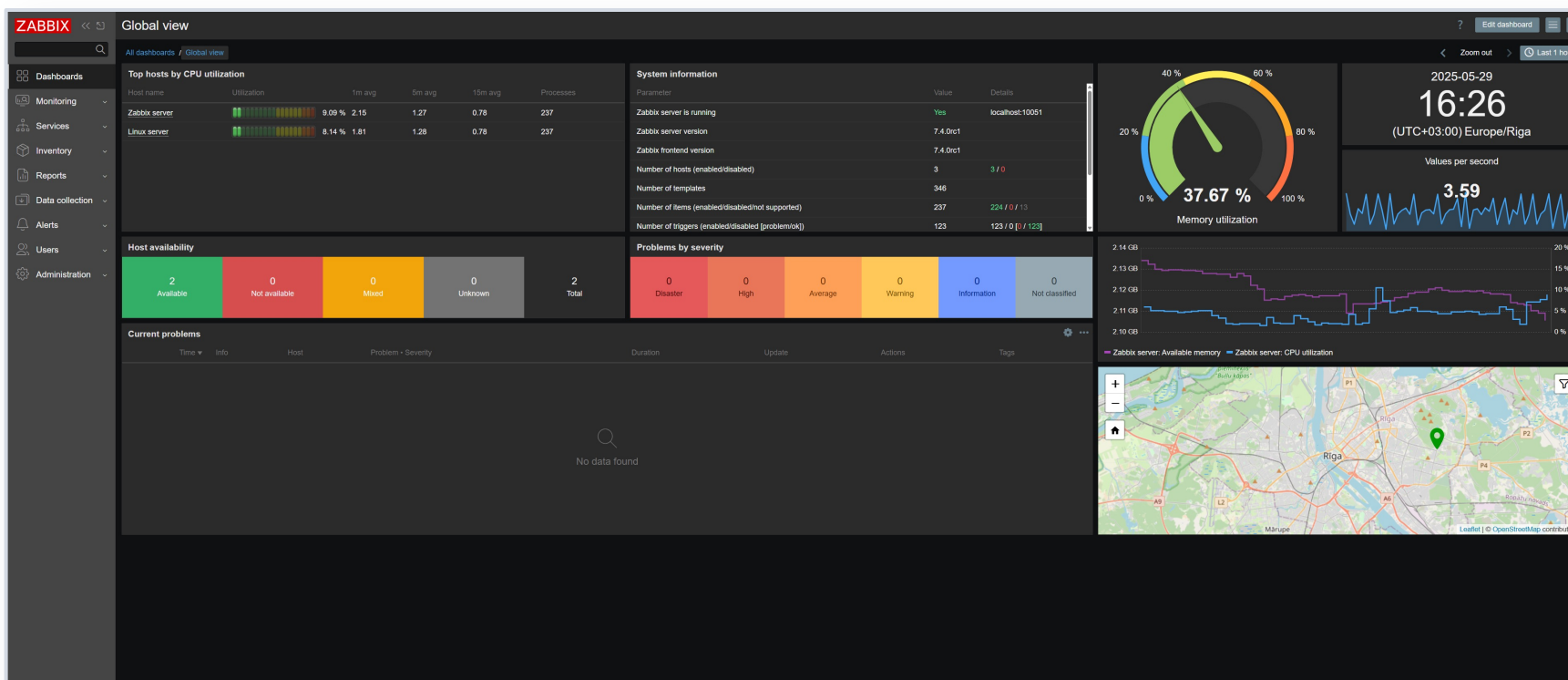
- ▶ New palette color schemes can be used for data sets in graphs, making the individual items more distinguishable
- ▶ Widget configuration changes are now instantly reflected in the widget without having to close the configuration form



Dashboard improvements

Various dashboard improvements to facilitate faster and smoother dashboard configuration

- ▶ The Global view default dashboard has received various improvements



7

Inline form validation

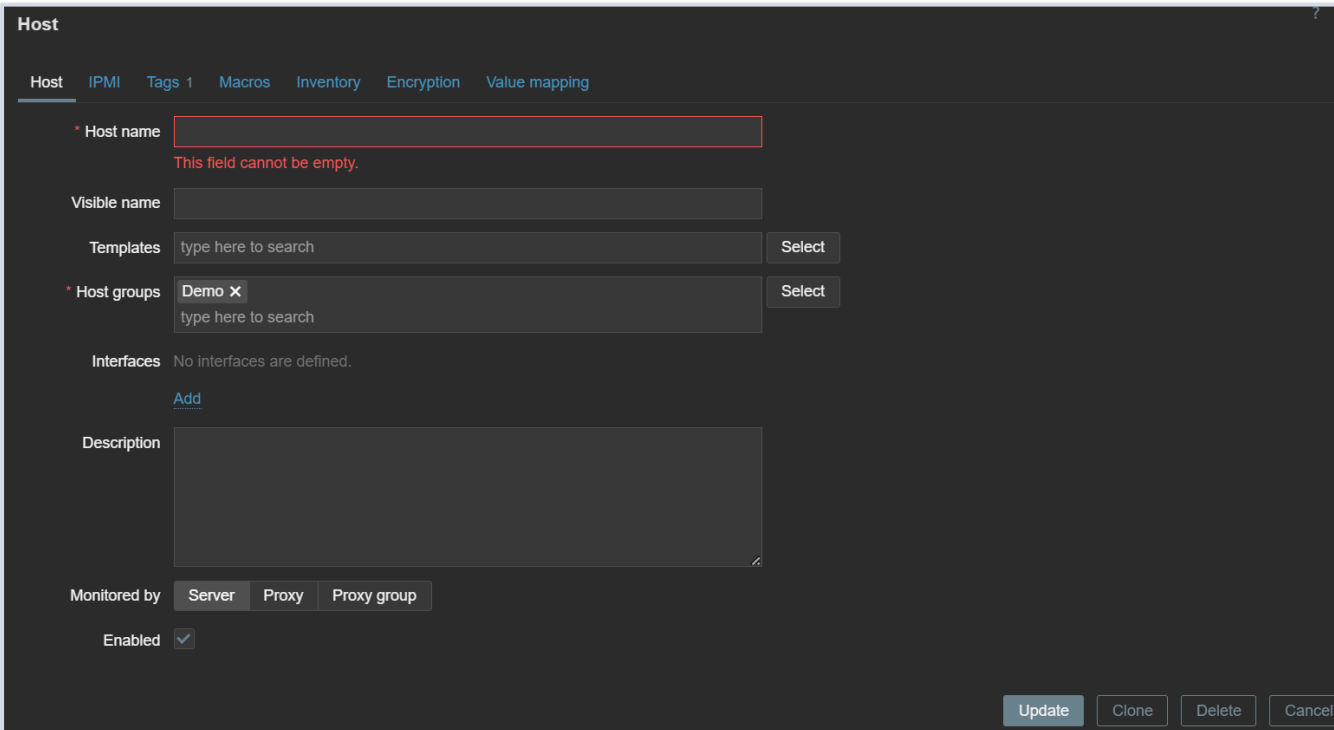


Inline form validation

As of 7.4, inline form validation is supported in:

- ▶ Host configuration
- ▶ Template configuration
- ▶ Item configuration
- ▶ Trigger configuration

Inline form validation support for other Zabbix sections is planned to be added in later major releases



The screenshot displays the 'Host' configuration form in Zabbix. The 'Host name' field is empty and has a red border with the error message 'This field cannot be empty.' below it. Other fields like 'Visible name', 'Templates', 'Host groups' (with a 'Demo' tag), 'Description', and 'Enabled' (checked) are visible. The 'Monitored by' section shows 'Server', 'Proxy', and 'Proxy group' buttons. The bottom right contains 'Update', 'Clone', 'Delete', and 'Cancel' buttons.

8

Frontend to server
communication encryption



Frontend to server communication encryption

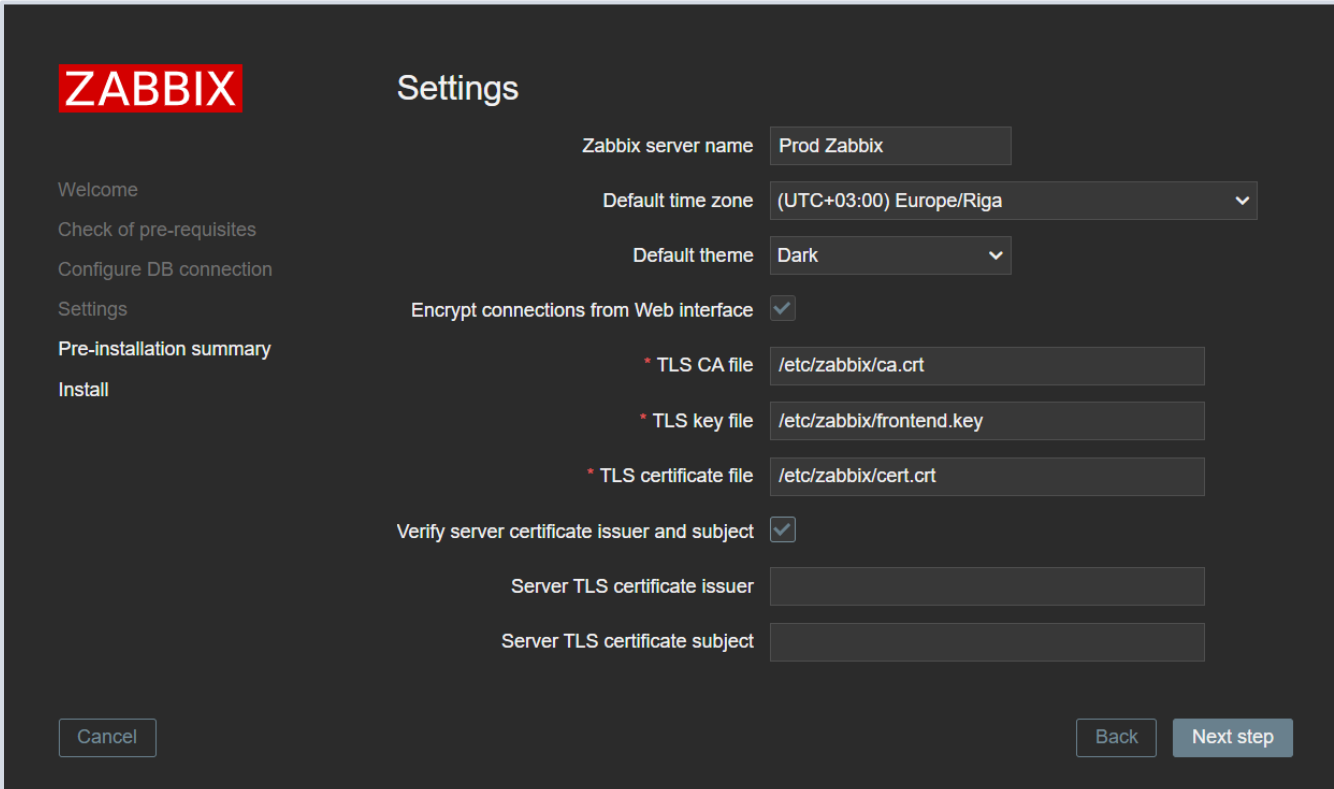
It is now possible to secure frontend to server communication with certificate encryption

New Zabbix server configuration parameters:

- ▶ *TLSFrontendAccept* – what incoming connections to accept from frontend
- ▶ *TLSFrontendCertIssuer* – Allowed frontend certificate issuer
- ▶ *TLSFrontendCertSubject* – Allowed frontend certificate subject
- ▶ *FrontendAllowedIP* – Frontend connections will be accepted only from addresses listed here if the parameter is set

Frontend to server communication encryption

It is now possible to secure frontend to server communication with certificate encryption



The screenshot shows the ZABBIX Settings page. On the left is a sidebar with navigation links: Welcome, Check of pre-requisites, Configure DB connection, Settings (highlighted), Pre-installation summary, and Install. The main content area is titled 'Settings' and contains the following configuration options:

- Zabbix server name: Prod Zabbix
- Default time zone: (UTC+03:00) Europe/Riga
- Default theme: Dark
- Encrypt connections from Web interface: ☒
- * TLS CA file: /etc/zabbix/ca.crt
- * TLS key file: /etc/zabbix/frontend.key
- * TLS certificate file: /etc/zabbix/cert.crt
- Verify server certificate issuer and subject: ☒
- Server TLS certificate issuer: (empty field)
- Server TLS certificate subject: (empty field)

At the bottom, there are three buttons: 'Cancel', 'Back', and 'Next step'.

9

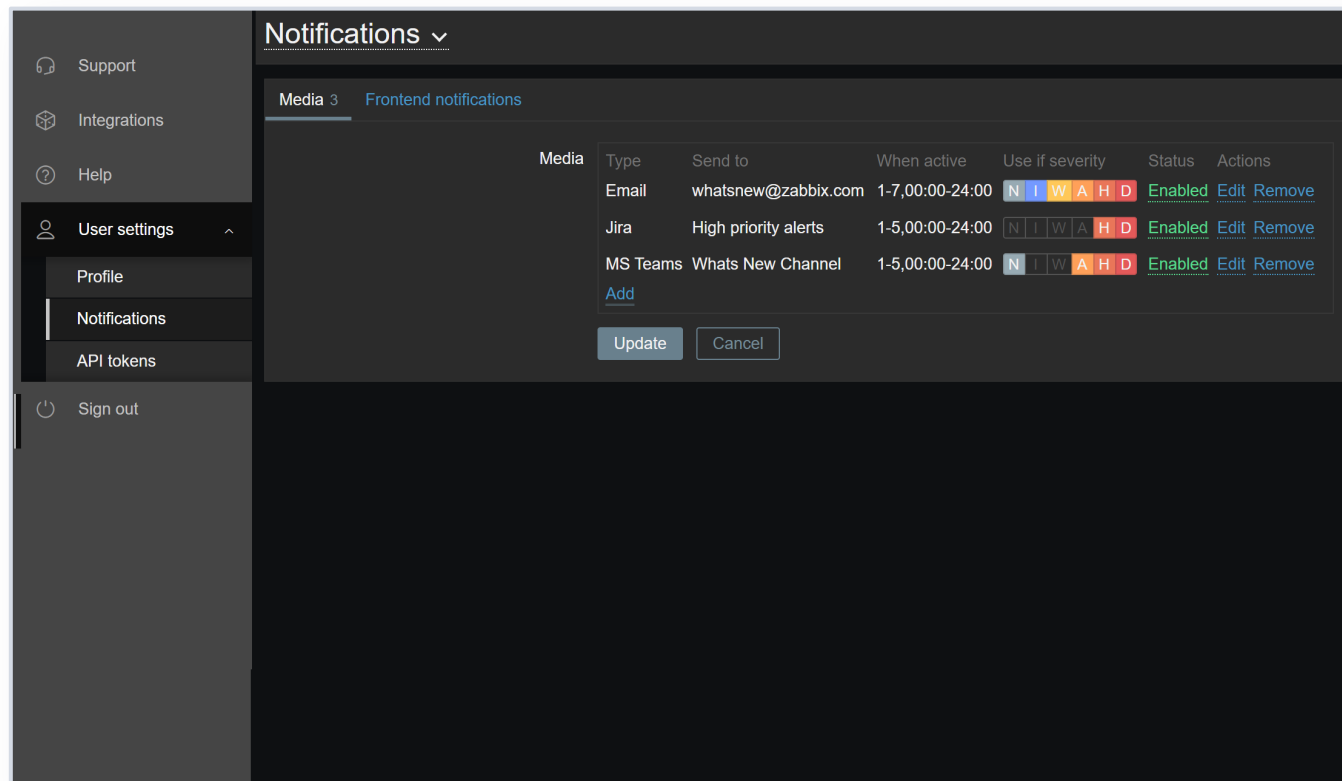
UX/UI improvements



General UI/UX improvements

Multiple UI/UX improvements have been added to improve existing Zabbix workflows:

- ▶ New Notifications section has been added under User Settings for customizing notification settings for the current user
- ▶ All users are now allowed to manage their own media by default. These permissions can now be revoked in user role settings
- ▶ Preprocessing results can now be copied directly to clipboard by using the Copy to clipboard button



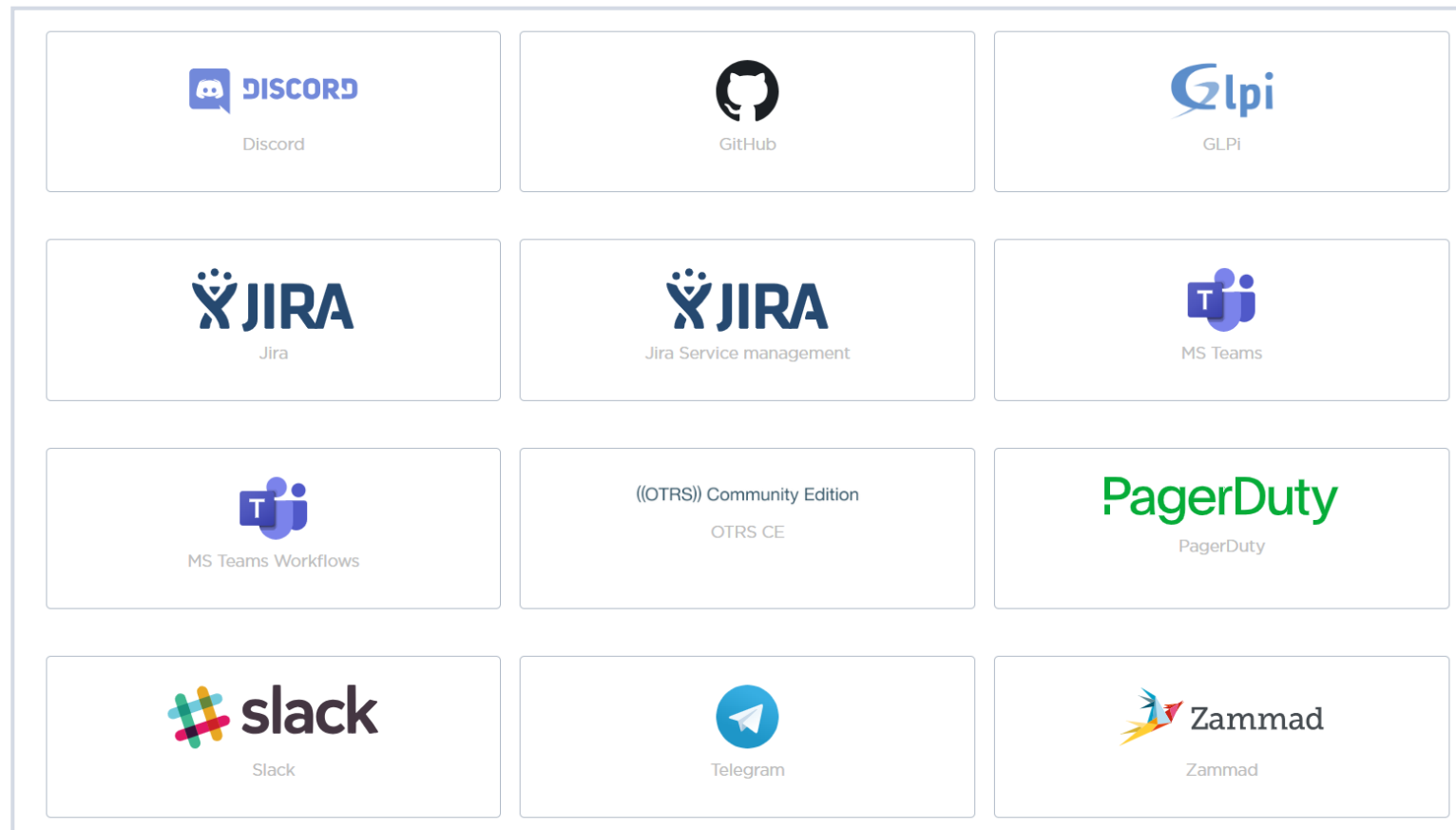
10

New templates and integrations



Existing webhook improvements

The following webhooks have been refactored and updated:



New templates



Pure Storage FlashArray by HTTP



Azure SQL Managed Instance by HTTP



Azure MSSQL DTU database by HTTP



Azure Backup Jobs by HTTP



Palo Alto PA-440 by HTTP



Juniper MX by NETCONF



Improvements and fixes for Dell by HTTP and SNMP

11

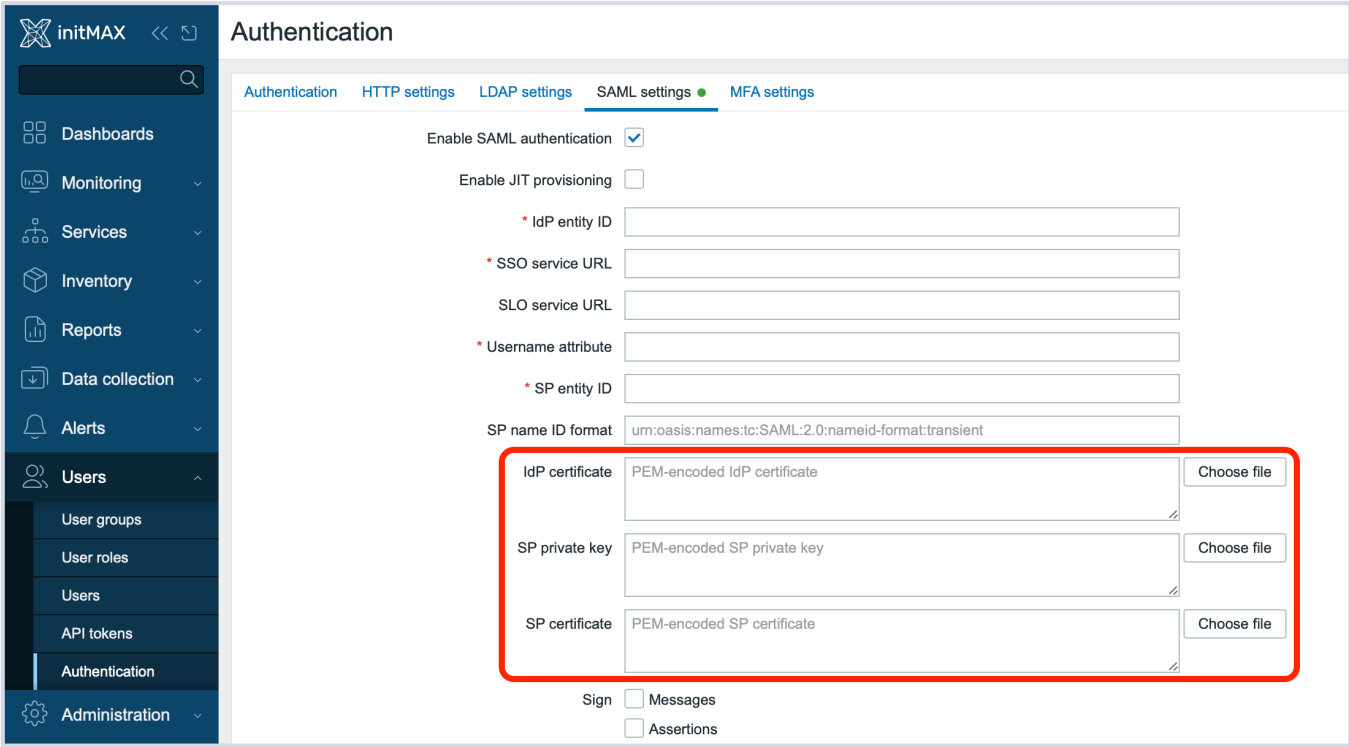
Store SAML certificates in the database



Store SAML certificates in the database

You can now configure Zabbix to store SAML certificates directly in the database.

- ▶ Easy configuration directly via the web interface.
- ▶ Unified certificate management in High Availability (HA) deployments.
- ▶ Simplified administration of the entire SAML configuration.



The screenshot displays the 'Authentication' configuration page in the initMAX web interface. The left sidebar contains a navigation menu with options: Dashboards, Monitoring, Services, Inventory, Reports, Data collection, Alerts, Users, and Administration. The 'Users' section is expanded, showing sub-items: User groups, User roles, Users, API tokens, Authentication, and Administration. The main content area is titled 'Authentication' and includes tabs for Authentication, HTTP settings, LDAP settings, SAML settings (active), and MFA settings. Under 'SAML settings', there are checkboxes for 'Enable SAML authentication' (checked) and 'Enable JIT provisioning' (unchecked). Below these are input fields for 'IdP entity ID', 'SSO service URL', 'SLO service URL', 'Username attribute', and 'SP entity ID'. The 'SP name ID format' is set to 'urn:oasis:names:tc:SAML:2.0:nameid-format:transient'. A red rectangular box highlights the certificate configuration section, which includes three rows: 'IdP certificate' with a 'Choose file' button, 'SP private key' with a 'Choose file' button, and 'SP certificate' with a 'Choose file' button. At the bottom, there are checkboxes for 'Sign' (unchecked), 'Messages' (unchecked), and 'Assertions' (unchecked).

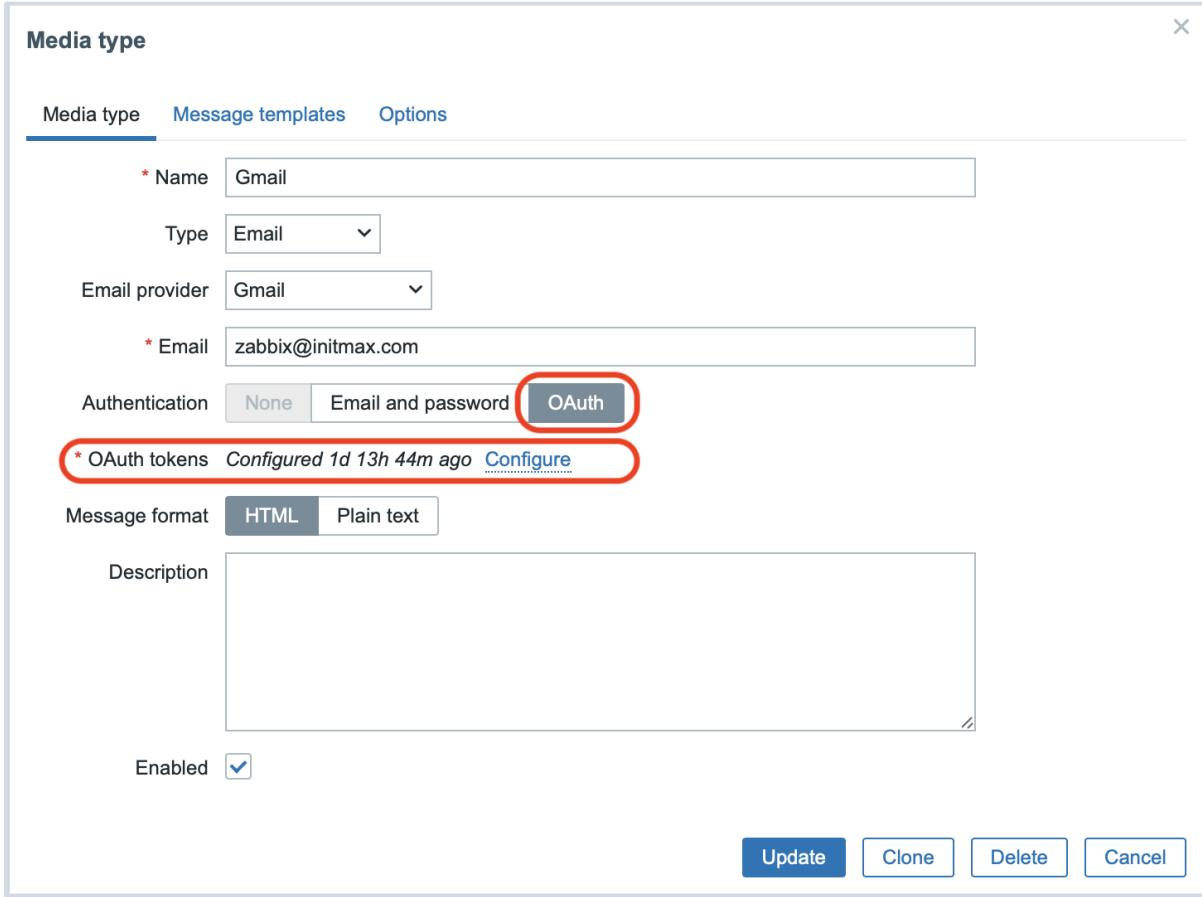
12

OAuth2 support for SMTP media



OAuth2 support for SMTP media

Zabbix now supports OAuth2 authentication for SMTP media types **Generic**, **Gmail**, and **Microsoft**.



The screenshot shows the 'Media type' configuration window in Zabbix. The 'Media type' tab is selected, showing the following fields:

- Name:** Gmail
- Type:** Email
- Email provider:** Gmail
- Email:** zabbix@initmax.com
- Authentication:** None, Email and password, **OAuth** (highlighted with a red circle)
- * OAuth tokens:** Configured 1d 13h 44m ago [Configure](#) (highlighted with a red circle)
- Message format:** HTML, Plain text
- Description:** (empty text area)
- Enabled:** ☒

At the bottom right, there are four buttons: Update, Clone, Delete, and Cancel.

13

History syncer detailed statistics



History syncer detailed statistics

History syncer processes now display detailed statistics about processed transactions directly in their names. This enables you to easily monitor how many values and triggers were processed and the duration of each operation.

- ▶ The notation “**A+B triggers**” means:
 - A**: triggers processed based on new values.
 - B**: triggers processed based on timers.
- ▶ In parentheses, you’ll find detailed timing of individual steps in the following order:
 - Time spent writing item values to the database
 - Time spent updating items (status, errors, host inventory, etc.)
 - Time spent writing trends to the database
 - Time spent calculating triggers
 - Time spent processing events and actions

```
/usr/local/sbin/zabbix_server: history syncer #1 [processed 1 values, 0+0 triggers in 0.001013 (0.001,0.000,0.000,0.000,0.000) sec, idle 1 sec]  
/usr/local/sbin/zabbix_server: history syncer #2 [processed 0 values, 0+0 triggers in 0.000025 (0.000,0.000,0.000,0.000,0.000) sec, idle 1 sec]  
/usr/local/sbin/zabbix_server: history syncer #3 [processed 0 values, 0+0 triggers in 0.000038 (0.000,0.000,0.000,0.000,0.000) sec, idle 1 sec]  
/usr/local/sbin/zabbix_server: history syncer #4 [processed 0 values, 0+0 triggers in 0.000031 (0.000,0.000,0.000,0.000,0.000) sec, idle 1 sec]
```

14

Additional changes and improvements



Additional changes and improvements

- ▶ Vault secret macros can now be resolved either by the Zabbix server or Zabbix proxy
- ▶ A new **icmppingretry** simple check has been added to monitor host responses to ICMP ping with the ability to modify retries
- ▶ New timestamp tracking history functions have been added
- ▶ Multiple new macros added for item-value time tracking
- ▶ Zabbix server/proxy automatically logs history cache diagnostic information when history cache is full
- ▶ Disabled items are now immediately removed from history cache
- ▶ It is now possible to manually clear history cache for a specific item by its id with `history_cache_clear=target` runtime command
- ▶ More detailed info can be found here:
<https://www.initmax.com/zabbix-7-4-is-here/> EN
<https://www.initmax.cz/novy-zabbix-7-4-je-zde/> CZ

Demo



Questions?



Contact us:

Phone:



+420 800 244 442

Web:



<https://www.initmax.com>

Email:



tomas.hermanek@initmax.cz

LinkedIn:



<https://www.linkedin.com/company/initmax>

Twitter:



<https://twitter.com/initmax>

Tomáš Heřmánek:



+420 732 447 184