

EVIDEN

BullSequana Servers

MONGUI User's Guide

The following copyright notice protects this book under Copyright laws which prohibit such actions as, but not limited to, copying, distributing, modifying, and making derivative works.

Copyright ©Bull SAS 2024, part of Eviden group. Eviden is a registered trademark of Eviden SAS. This document, or any part of it, may not be reproduced, copied, circulated and/or distributed nor quoted without prior written approval from Bull SAS.

Trademarks and Acknowledgements

We acknowledge the right of proprietors of trademarks mentioned in this manual.

All brand names and software and hardware product names are subject to trademark and/or patent protection.

Quoting of brand and product names is for information purposes only and does not represent trademark and/or patent misuse.

Hardware

September 2024

**Eviden
30 bis rue du Nid de Pie
49000 Angers
FRANCE**

The information in this document is subject to change without notice. Eviden will not be liable for errors contained herein, or for incidental or consequential damages in connection with the use of this material.

Table of Contents

Preface	p-1
Intended Readers	p-1
Chapter 1. Installing MONGUI	1-1
1.1. Overview	1-1
1.2. Installing MONGUI	1-2
1.3. Delivery content	1-3
Chapter 2. Getting started with MONGUI	2-1
2.1. Setting proxy configuration	2-1
2.2. Starting the Zabbix console	2-2
2.3. Installing the scripts	2-4
Chapter 3. Managing templates	3-1
3.1. Installing the template	3-1
3.2. Check the templates version	3-3
3.3. Template content	3-4
Chapter 4. Managing hosts	4-1
4.1. Installing the Hosts template	4-1
4.2. Adding a host using the Hosts template	4-3
4.3. Adding a host manually	4-6
4.3.1. Creating a host	4-6
4.3.2. Linking a host to the template	4-8
4.3.3. Adding macros on a host	4-11
Chapter 5. Monitoring rsyslog	5-1
Chapter 6. Customizing the Zabbix console	6-1
6.1. Creating a dashboard	6-1
6.2. Adding a graph to a dashboard	6-2
6.3. Adding a predefined graph prototype to a dashboard	6-5
6.4. Adding a plain text to a dashboard	6-8
6.5. Adding a map	6-11
Chapter 7. Setting up emails alerts	7-1
7.1. Configuring an email media	7-1

7.2. Adding an email media for a user or a user group	7-3
7.3. Creating a trigger action	7-7

Preface

This guide explains how to use the MONitoring Graphical User Interface (MONGUI) to manage BullSequana servers.

See The Bull support web site for the most up to date product information, documentation, firmware updates, software fixes and service offers:
<https://support.bull.com>

Intended Readers

This guide is intended for use by system administrators and operators.

Chapter 1. Installing MONGUI

1.1. Overview

The MONitoring Graphical User Interface (MONGUI) can be used to monitor multiple BullSequana SH, BullSequana EX or BullSequana S servers. The MONGUI package provides Zabbix templates with their associated scripts.

1.2. Installing MONGUI

This section explains how to install and update MONGUI on the system selected to host it.

Prerequisites

- The MONGUI_<version>.tar.gz package is available
- The following packages are installed:
 - Zabbix version 5.0 or higher
 - Python version 3.7 or higher
- Zabbix is installed and running

Procedure

1. Open a terminal window.
2. Go to the installation directory.
3. Extract the MONGUI file:

```
tar xzvf MONGUI-<version>.tar.gz
```

The templates are delivered in a sub-directory of the installation directory:
<install_dir>\zabbix\server\externalscripts.

1.3. Delivery content

On delivery, MONGUI contains:

- Two templates that allow Zabbix to be used to monitor BullSequana SH, BullSequana EX or BullSequana S servers:
 - template_<server_range>_zbxv5.xml
 - template_<server-range>_Hosts-zbxv5.xml

Where <server_range> can take the following values:

- BullSequanaSH for BullSequana SH servers
 - BullSequanaEdge for BullSequana EX servers
 - BullSequanaSeries for BullSequana S servers
- A set of scripts that allow to discover sensors and collect information

Chapter 2. Getting started with MONGUI

To monitor systems, the MONitoring Graphical User Interface (MONGUI) uses Zabbix. Zabbix is an enterprise-class open source distributed monitoring solution accessible via a web-based interface.

See The full Zabbix documentation
<https://www.zabbix.com/documentation/current/en/manual>

2.1. Setting proxy configuration

The proxy variables are automatically copied in zabbix environment.

1. Edit the proxy configuration file.

Default: /etc/systemd/proxy.sh

2. Check the proxy variables.

```
export HTTP_PROXY=http://<proxy>:<port number>
export HTTPS_PROXY=https://<proxy>:<port number>
export NO_PROXY=127.0.0.1,localhost,<IP address>
```

```
export http_proxy=http://<proxy>:<port number>
export https_proxy=https://<proxy>:<port number>
export no_proxy=127.0.0.1,localhost,<IP address>
```

3. Set the variables as required.

2.2. Starting the Zabbix console

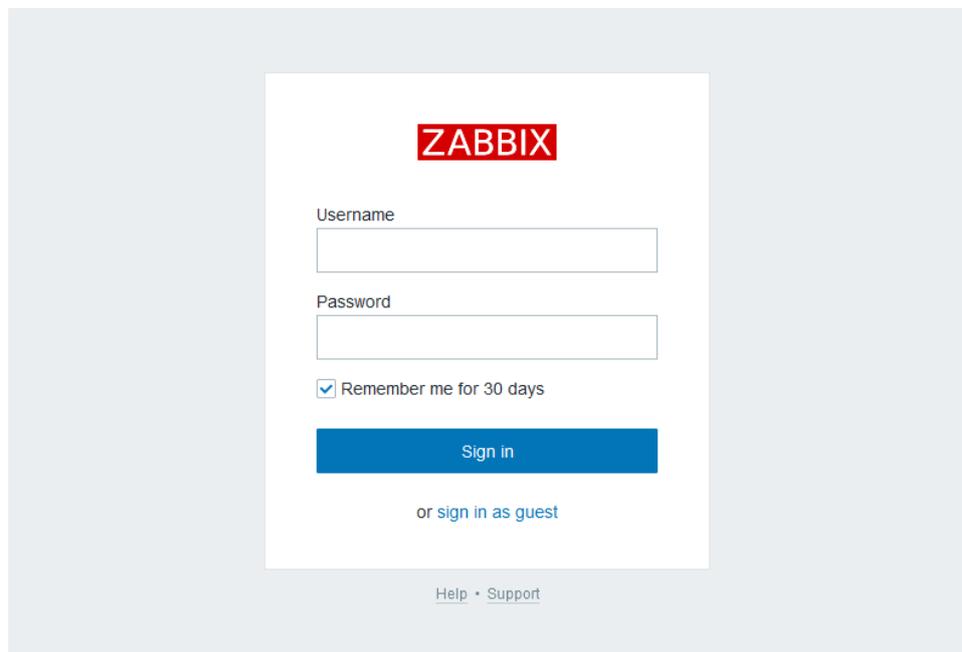
Prerequisite

Zabbix is running

Procedure

1. Open a web browser.
2. Connect to the Zabbix console by entering the name or IP address of the Zabbix console followed by the port number in the address bar, using the https protocol.

The authentication page opens.



Zabbix console	
Username	Default: Admin
Password	Default: zabbix

3. Complete the **Username** and **Password** fields.
4. Click **Log In**. The **Dashboard** page opens.

Important It is strongly recommended to change the default user password once initial setup is completed, taking care to record the new account details for subsequent connections.

What to do if an incident occurs?

If the connection to the console cannot be made or if the web pages are displayed incorrectly, one of the following problems may be the cause:

- Network failure
- Incorrect network settings
- Incorrect browser settings (proxy configuration)

2.3. Installing the scripts

Data collection is performed by the Zabbix server using Python scripts.

1. Edit the Zabbix server configuration file `/etc/zabbix/zabbix_server.conf`.
2. Check the **ExternalScripts** parameter.
This parameter defines the location for external scripts.
Default: `/usr/lib/zabbix/externalscripts`
3. Copy the scripts in the ExternalScripts directory.

Important In the ExternalScripts directory, another directory named **openbmc** must be created with read and write permissions.

Available scripts

BullSequana SH and BullSequana EX servers

Script name	Description
<code><server_type>_openbmc_discovery</code>	Discovers enumerables like sensors
<code><server_type>_openbmc_frus_collect</code>	Collects FRU information
<code><server_type>_openbmc_frus_discovery</code>	Discovers enumerables like FRU
<code><server_type>_openbmc_frus_reader</code>	Reads FRU information previously collected
<code><server_type>_openbmc_fw_collect</code>	Collects firmware information
<code><server_type>_openbmc_fw_reader</code>	Reads firmware information previously collected
<code><server_type>_openbmc_network_collect</code>	Collects network information
<code><server_type>_openbmc_network_discovery</code>	Discovers enumerables like network
<code><server_type>_openbmc_network_reader</code>	Reads network information previously collected
<code><server_type>_openbmc_sensors_collect</code>	Collects sensors information
<code><server_type>_openbmc_sensors_reader</code>	Reads sensors information previously collected
<code><server_type>_openbmc_system_collect</code>	Collects system information
<code><server_type>_openbmc_system_reader</code>	Reads system information previously collected

Where `<server_type>` can take the following values:

- `mesca5` for BullSequana SH servers
- `ora` for BullSequana EX servers

BullSequana S servers

Script name	Description
mesca3_openbmc_discovery	Discovers enumerables like sensors
mesca3_openbmc_sensors_reader	Reads sensors information previously collected
ipmitoolsSensors	Collects sensors information

Important The run time of the ipmitoolsSensors script may exceed the maximum value configurable. A workaround is to execute the script via the crontab every two minutes.

Chapter 3. Managing templates

Important It is strongly recommended not to modify the original templates. Copy the originals or create templates instead.

The server template is a set of entities (items, triggers, graphs, discovery rules) allowing efficient management of its devices.

The available MONGUI templates are `template_<server_model>_zbxv5.xml` where `<server_type>` can take the following values:

- BullSequanaSH for BullSequana SH servers
- BullSequanaEdge for BullSequana EX servers
- BullSequanaSeries for BullSequana S servers

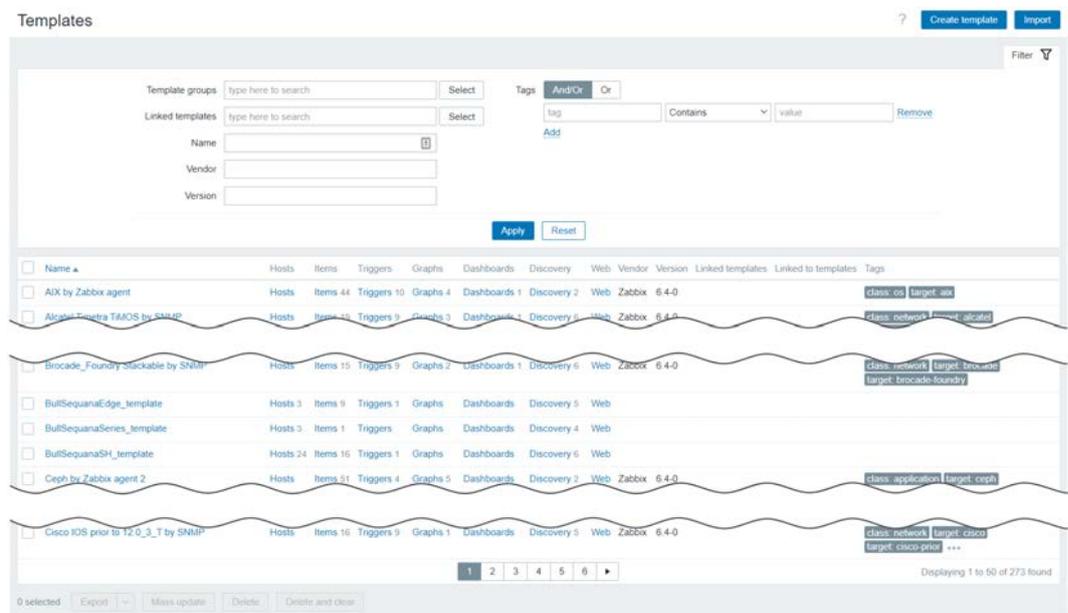
3.1. Installing the template

Prerequisites

The `template_<server_model>_zbxv5.xml` file is copied from `<install_dir>\zabbix\server\externalscripts\` in a local directory on the client computer running the browser.

Procedure

1. From the **Data collection** menu, click the **Templates** tab. The **Templates** page opens.



2. Click **Import** at the top right of the page. The **Import** page opens.

Import ? X

* Import file Aucun fichier choisi

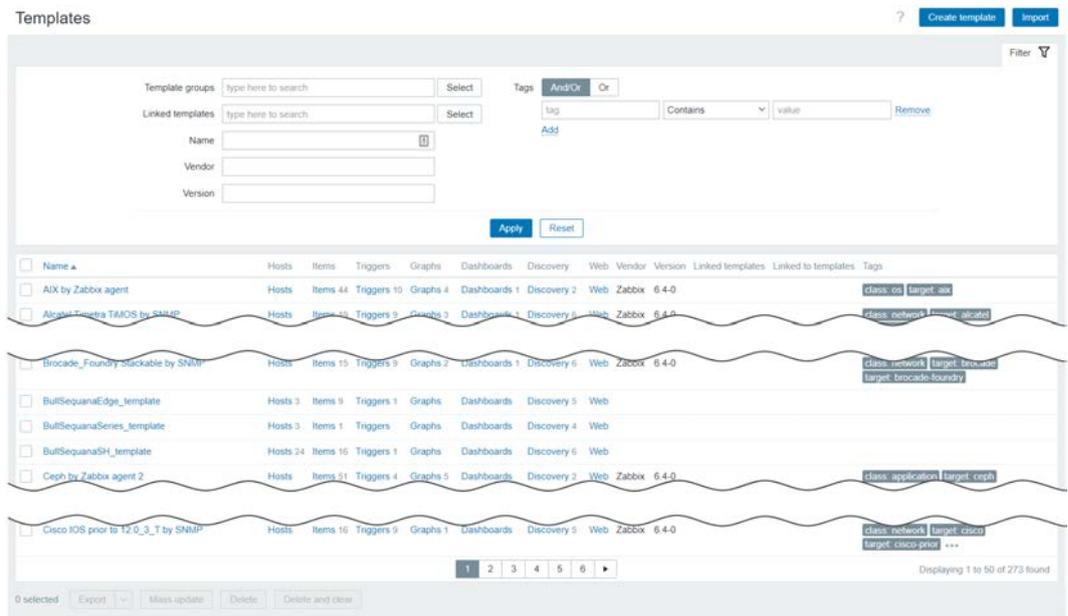
Advanced options

Rules	Update existing	Create new	Delete missing
All	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Template groups	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Host groups	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Templates	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Value mappings	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Template dashboards	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Template linkage		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Items	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Discovery rules	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Triggers	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Graphs	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Web scenarios	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

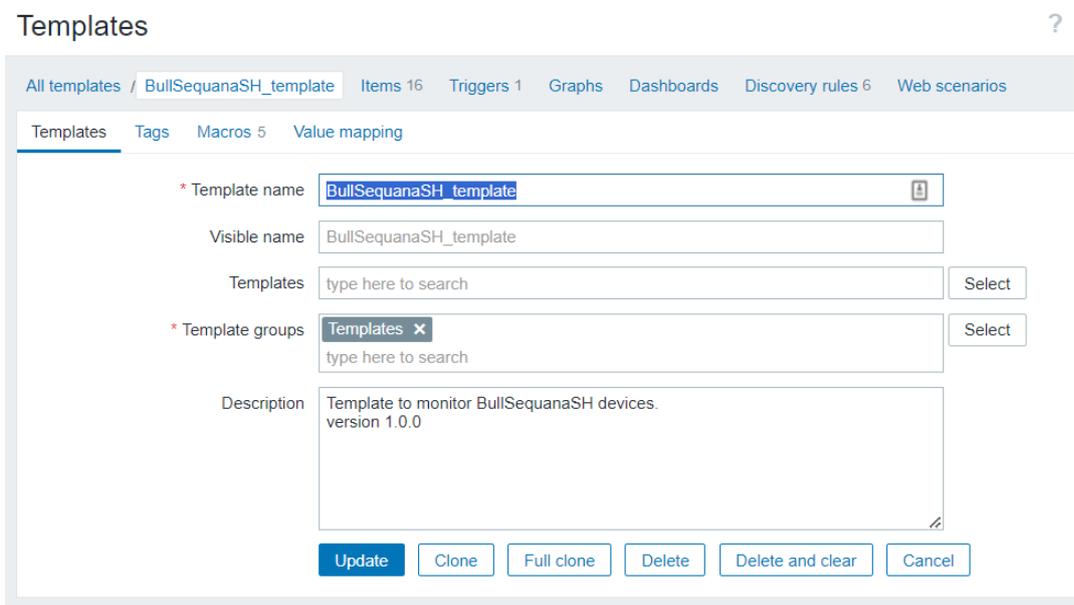
3. In the **Import file** field, click **Choose File** and indicate the path to the template.
4. Click **Import**.

3.2. Check the templates version

1. From the **Data collection** menu, click the **Templates** tab. The **Templates** page opens.



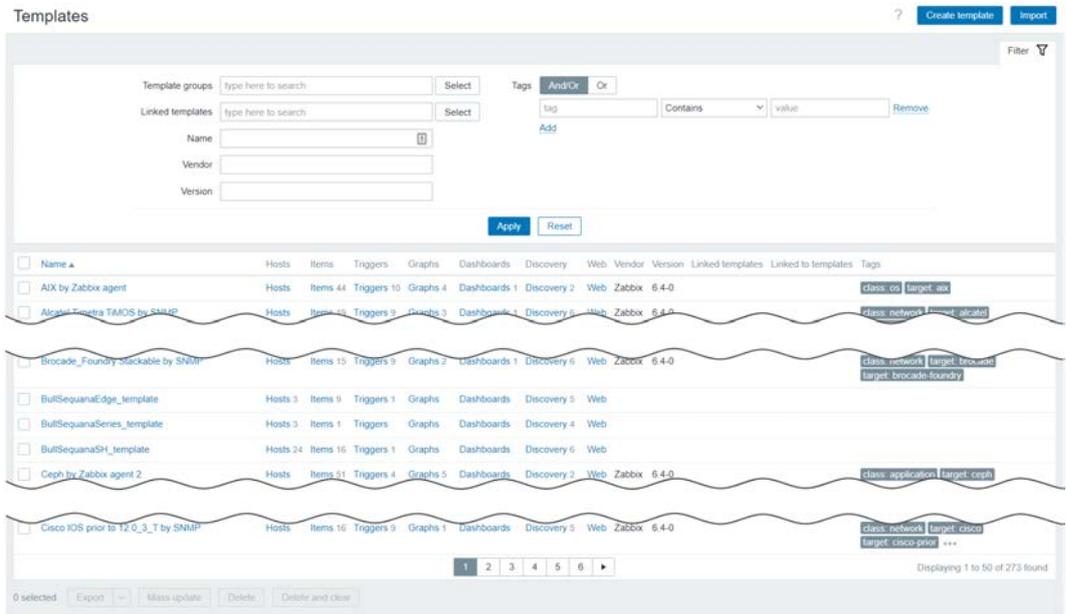
2. Select the <server_model>_template to check.



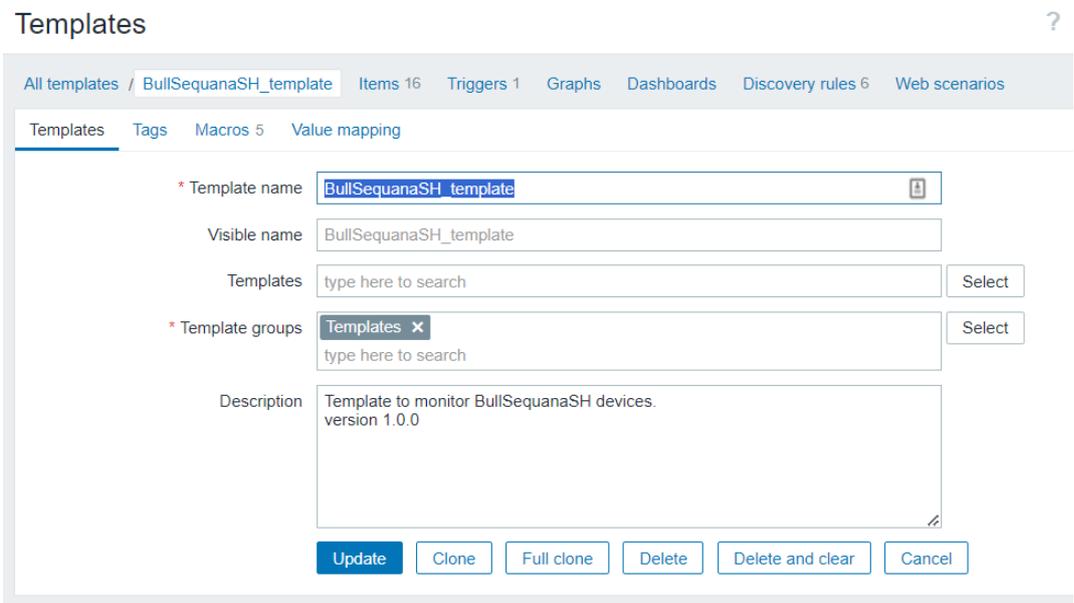
3. Check the version.

3.3. Template content

1. From the **Data collection** menu, click the **Templates** tab. The **Templates** page opens.



2. Click a <server_model>_template name in the list. A new page opens.



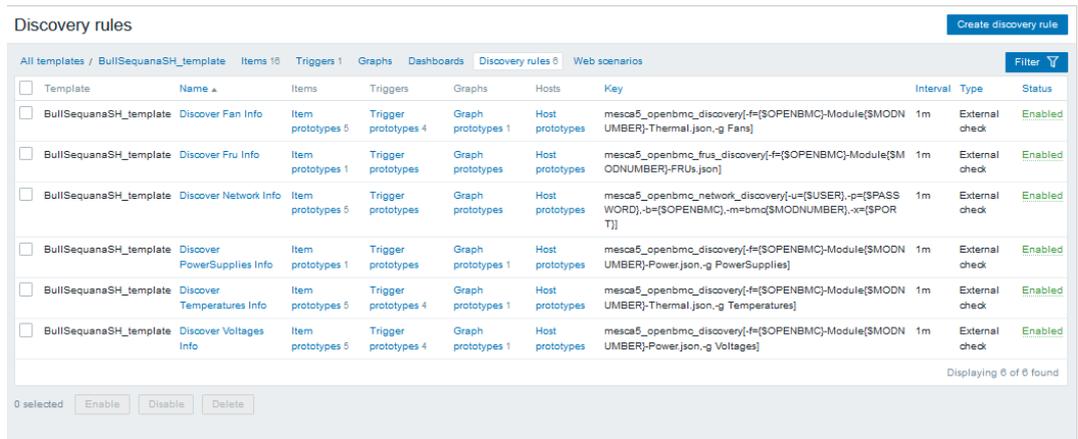
3. Click the **Items** tab. A new page opens.

Name	Triggers	Key	Interval	History	Trends	Type	Status	Tags
System_serialNumber		mesca5_openbmc_system_reader[-f={SOPENBMC}-system.json.-p=SerialNumber]	10m	7d		External check	Enabled	
System_partNumber		mesca5_openbmc_system_reader[-f={SOPENBMC}-system.json.-p=PartNumber]	10m	7d		External check	Enabled	
System_model		mesca5_openbmc_system_reader[-f={SOPENBMC}-system.json.-p=Model]	10m	7d		External check	Enabled	
System_manufacturer		mesca5_openbmc_system_reader[-f={SOPENBMC}-system.json.-p=Manufacturer]	10m	7d		External check	Enabled	
System_collect		mesca5_openbmc_system_collect[-u={USER}.-p={PASSWORD}.-b={SOPENBMC}.-x={SPORT}]	10m	0		External check	Enabled	
Thermal_collect		mesca5_openbmc_sensors_collect[-u={USER}.-p={PASSWORD}.-b={SOPENBMC}.-x={SPORT}.-m=Module{SMODNUMBER}.-f=Thermal]	10m	0		External check	Enabled	
Power_collect		mesca5_openbmc_sensors_collect[-u={USER}.-p={PASSWORD}.-b={SOPENBMC}.-x={SPORT}.-m=Module{SMODNUMBER}.-f=Power]	10m	0		External check	Enabled	
CEB_P_CPLD_version		mesca5_openbmc_fw_reader[-f={SOPENBMC}-Module{MODNUMBER}-firmwares.json.-i=CEB_P_CPLD.-p=Version]	10m	7d		External check	Enabled	
CEB_MAIN_FPGA_version		mesca5_openbmc_fw_reader[-f={SOPENBMC}-Module{MODNUMBER}-firmwares.json.-i=CEB_MAIN_FPGA.-p=Version]	10m	7d		External check	Enabled	
CEB_IO_FPGA_version		mesca5_openbmc_fw_reader[-f={SOPENBMC}-Module{MODNUMBER}-firmwares.json.-i=CEB_IO_FPGA.-p=Version]	10m	7d		External check	Enabled	
BMC_version	Triggers 1	mesca5_openbmc_fw_reader[-f={SOPENBMC}-Module{MODNUMBER}-firmwares.json.-i=BMC.-p=Version]	10m	7d		External check	Enabled	
BMC_state		mesca5_openbmc_fw_reader[-f={SOPENBMC}-Module{MODNUMBER}-firmwares.json.-i=BMC.-p=Status.-s=State]	10m	7d		External check	Enabled	
BIOS_version		mesca5_openbmc_fw_reader[-f={SOPENBMC}-Module{MODNUMBER}-firmwares.json.-i=BIOS.-p=Version]	10m	7d		External check	Enabled	
BIOS_state		mesca5_openbmc_fw_reader[-f={SOPENBMC}-Module{MODNUMBER}-firmwares.json.-i=BIOS.-p=Status.-s=State]	10m	7d		External check	Enabled	
Firmwares_collect		mesca5_openbmc_fw_collect[-u={USER}.-p={PASSWORD}.-b={SOPENBMC}.-m=Module{MODNUMBER}.-x={SPORT}]	10m	0		External check	Enabled	
Frus_collect		mesca5_openbmc_frus_collect[-u={USER}.-p={PASSWORD}.-b={SOPENBMC}.-m=Module{MODNUMBER}.-x={SPORT}]	10m	90d		External check	Enabled	

The items execute the external scripts provided by MONGUI. Some items are used to collect information, others are used to read specific data previously collected.

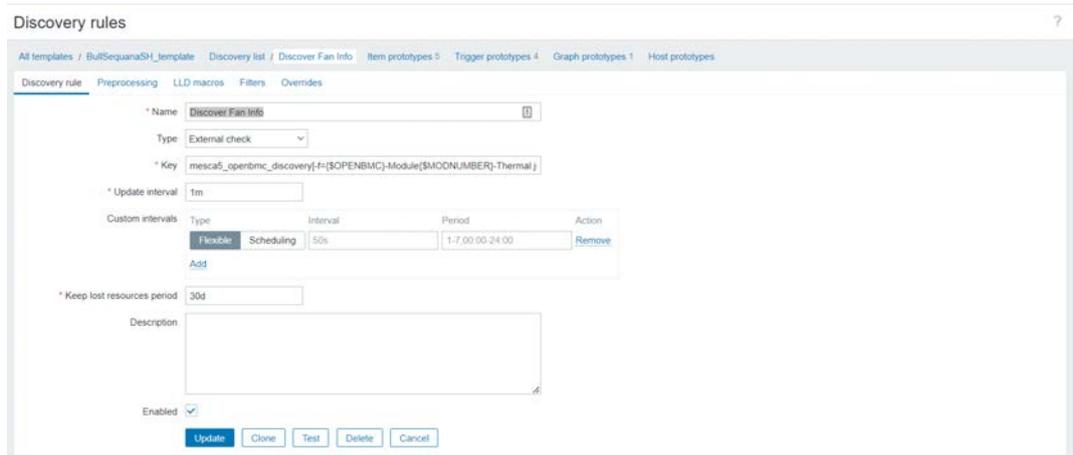
Note BullSequana S server has only one item to collect information from sensors.

- Click the **Discovery rules** tab. A new page opens.

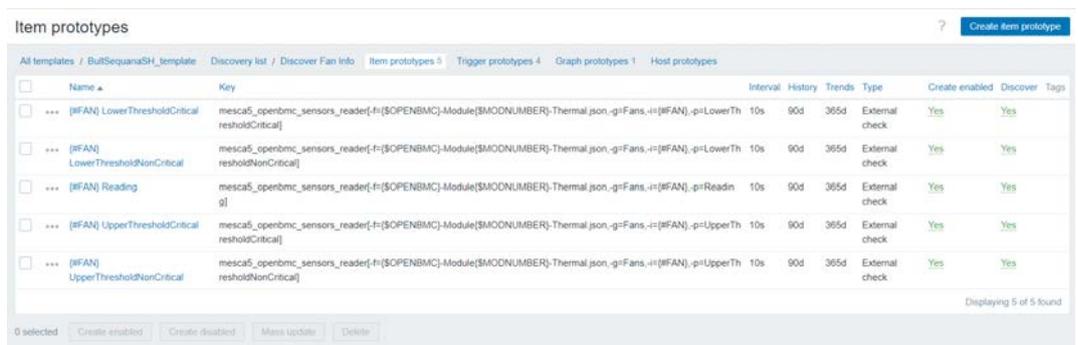


Discovery rules provide a way to automatically create items, triggers and graphs for different entities (Fans, Temperatures, Voltages...).

- Click a Discovery rule name in the list. A new page opens.



- Click **Item prototypes** tab to see the discovered items.



- Click **Trigger prototypes** tab to see the discovered triggers.

For BullSequana EX and BullSequana SH servers four trigger prototypes are displayed.

Trigger prototypes ? Create trigger prototype

Severity	Name	Operational data	Expression	Create enabled	Discover	Tags
High	{#FAN} lower critical threshold		last({BullSequanaSH_template/mesca5_openbmc_sensors_reader[-t-]{\$OPENBMC}Module{\$MOONNUMBER}Thermal.json,g=Fans,-i[#{FAN}],-p=Reading)}<-last({BullSequanaSH_template/mesca5_openbmc_sensors_reader[-t-]{\$OPENBMC}Module{\$MOONNUMBER}Thermal.json,g=Fans,-i[#{FAN}],-p=LowerThresholdCritical})	Yes	Yes	
Warning	{#FAN} lower non critical threshold		last({BullSequanaSH_template/mesca5_openbmc_sensors_reader[-t-]{\$OPENBMC}Module{\$MOONNUMBER}Thermal.json,g=Fans,-i[#{FAN}],-p=Reading)}<-last({BullSequanaSH_template/mesca5_openbmc_sensors_reader[-t-]{\$OPENBMC}Module{\$MOONNUMBER}Thermal.json,g=Fans,-i[#{FAN}],-p=LowerThresholdNonCritical})	Yes	Yes	
High	{#FAN} upper critical Threshold		last({BullSequanaSH_template/mesca5_openbmc_sensors_reader[-t-]{\$OPENBMC}Module{\$MOONNUMBER}Thermal.json,g=Fans,-i[#{FAN}],-p=Reading)}>=last({BullSequanaSH_template/mesca5_openbmc_sensors_reader[-t-]{\$OPENBMC}Module{\$MOONNUMBER}Thermal.json,g=Fans,-i[#{FAN}],-p=UpperThresholdCritical})	Yes	Yes	
Warning	{#FAN} upper non critical Threshold		last({BullSequanaSH_template/mesca5_openbmc_sensors_reader[-t-]{\$OPENBMC}Module{\$MOONNUMBER}Thermal.json,g=Fans,-i[#{FAN}],-p=Reading)}>=last({BullSequanaSH_template/mesca5_openbmc_sensors_reader[-t-]{\$OPENBMC}Module{\$MOONNUMBER}Thermal.json,g=Fans,-i[#{FAN}],-p=UpperThresholdNonCritical})	Yes	Yes	

0 selected Create enabled Create disabled Mass update Delete

For every sensor, critical high and low triggers, corresponding to critical alarm thresholds, as well as warning high and low triggers, corresponding to warning alarm thresholds for the devices are enabled by default.

For BullSequana S servers two trigger prototypes are displayed.

Trigger prototypes ? Create trigger prototype

Severity	Name	Operational data	Expression	Create enabled	Discover	Tags
High	{#FAN} lower critical threshold		last({BullSequanaSeries_template/mesca3_openbmc_sensors_reader[-t-]{\$OPENBMC}-ipmi-sensors.json,g=RPM,-i[#{FAN}],-p=Reading)}<-last({BullSequanaSeries_template/mesca3_openbmc_sensors_reader[-t-]{\$OPENBMC}-ipmi-sensors.json,g=RPM,-i[#{FAN}],-p=Lower C})	Yes	Yes	
High	{#FAN} upper critical Threshold		last({BullSequanaSeries_template/mesca3_openbmc_sensors_reader[-t-]{\$OPENBMC}-ipmi-sensors.json,g=RPM,-i[#{FAN}],-p=Reading)}>=last({BullSequanaSeries_template/sensors_reader[-t-]{\$OPENBMC}-ipmi-sensors.json,g=RPM,-i[#{FAN}],-p=Upper C})	Yes	Yes	

0 selected Create enabled Create disabled Mass update Delete

For every sensor, critical high and low triggers, corresponding to critical alarm thresholds for the devices are enabled by default.

- Click **Graph prototypes** tab to see the discovered graphs.

Graph prototypes ? Create graph prototype

Name	Width	Height	Graph type	Discover
{#FAN}	900	200	Normal	Yes

0 selected Delete

Chapter 4. Managing hosts

4.1. Installing the Hosts template

The Hosts template allows to add a host easily with a minimum of operations.

The available MONGUI Hosts templates are `template_<server_model>_Hosts-zbxv5.xml` where `<server_model>` can take the following values:

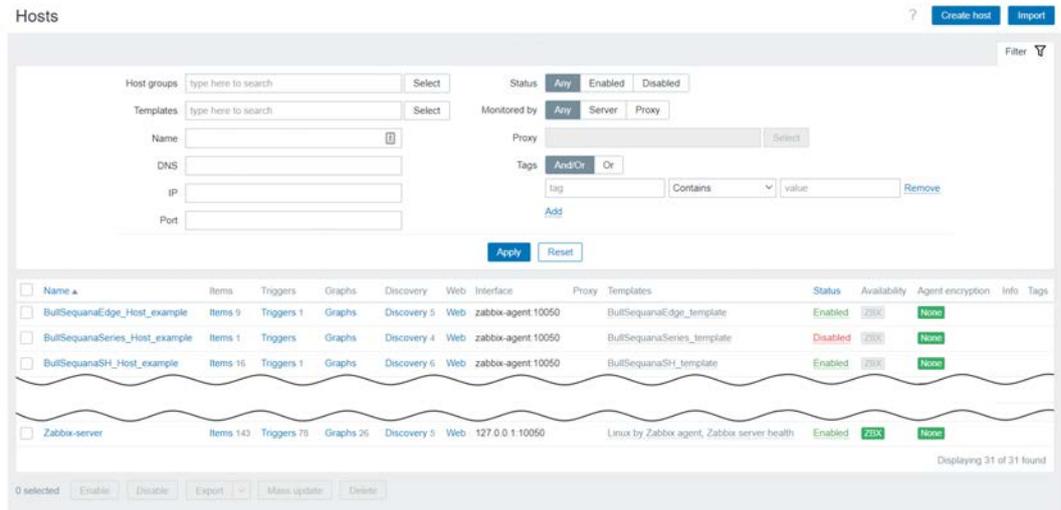
- BullSequanaSH for BullSequana SH servers
- BullSequanaEdge for BullSequana EX servers
- BullSequanaSeries for BullSequana S servers

Prerequisites

- The `<server_model>` template is imported
- The `template_<server_model>_Hosts-zbxv5.xml` file is copied from `<install_dir>\zabbix\server\externalscripts\` to a local directory on the client computer running the browser

Procedure

1. From the **Data collection** menu, click the **Hosts** tab. The **Hosts** page opens.



2. Click **Import**. The **Import** page opens.

Import ? x

* Import file Aucun fichier choisi

Advanced options

Rules	Update existing	Create new	Delete missing
All	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Host groups	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Hosts	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Value mappings	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Template linkage		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Items	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Discovery rules	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Triggers	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Graphs	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Web scenarios	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

3. In the **Import file** field, click **Choose File** and indicate the path to the template_<server_model>_Hosts-zbxv5.xml file.

4. Select **Hosts** check boxes.

5. Click **Import**. A <server_model>_Host_example host is created.

4.2. Adding a host using the Hosts template

The <server_model>_Host_example allows to automatically configure a host:

- The Zabbix agent is configured to zabbix-agent:10050
- Automatic Inventory is configured
- Macros are prepared
- The <server_model> template is linked

Procedure

1. From the **Data Collection** menu, click the **Hosts** tab. The **Hosts** page opens.

The screenshot displays the Zabbix Hosts management interface. At the top, there are search and filter options for Host groups and Templates. Below these are input fields for Name, DNS, IP, and Port. There are also buttons for 'Apply' and 'Reset'. The main part of the interface is a table of hosts. The table has columns for Name, Items, Triggers, Graphs, Discovery, Web, Interface, Proxy, Templates, Status, Availability, Agent encryption, Info, and Tags. The table lists three example hosts: BullSequanaEdge_Host_example, BullSequanaSeries_Host_example, and BullSequanaSH_Host_example, along with a 'Zabbix-server' host. At the bottom, there are buttons for '0 selected', 'Enable', 'Disable', 'Export', 'Mass update', and 'Delete'.

Name	Items	Triggers	Graphs	Discovery	Web	Interface	Proxy	Templates	Status	Availability	Agent encryption	Info	Tags
BullSequanaEdge_Host_example	Items 9	Triggers 1	Graphs	Discovery 5	Web	zabbix-agent 10050		BullSequanaEdge_template	Enabled	ZBX	None		
BullSequanaSeries_Host_example	Items 1	Triggers	Graphs	Discovery 4	Web	zabbix-agent 10050		BullSequanaSeries_template	Disabled	ZBX	None		
BullSequanaSH_Host_example	Items 16	Triggers 1	Graphs	Discovery 5	Web	zabbix-agent 10050		BullSequanaSH_template	Enabled	ZBX	None		
Zabbix-server	Items 143	Triggers 78	Graphs 26	Discovery 5	Web	127.0.0.1:10050		Linux by Zabbix agent, Zabbix server health	Enabled	ZBX	None		

2. Select a <server_model>_Host_example. A new page opens.

Host

Host IPMI Tags Macros 5 Inventory Encryption Value mapping

Visible name: BullSequanaSH_Host_example

Templates: Name Action
BullSequanaSH_template Unlink Unlink and clear

type here to search Select

* Host groups: Templates x type here to search Select

Interfaces: Type IP address DNS name Connect to Port Default
Agent zabbix-agent IP DNS 10050 Remove

Add

Description

Monitored by proxy: (no proxy)

Enabled:

Update Clone Full clone Delete Cancel

3. Click **Clone**.

4. Modify the **Host name**.

Note The host name may contain alphanumeric characters, spaces, dots, dashes and underscores. Leading and trailing spaces are not allowed.

5. Click the **Macros** tab.

Host

Host IPMI Tags Macros 5 Inventory Encryption Value mapping

Host macros Inherited and host macros

Macro	Value	Description
{\$MODNUMBER}	0	description
{\$OPENBMC}	XX.XX.XX.XX	description
{\$PASSWORD}	the_passwd	description
{\$PORT}	443	description
{\$USER}	the_user	description

Add

Update Clone Full clone Delete Cancel

6. Complete the macros as required.

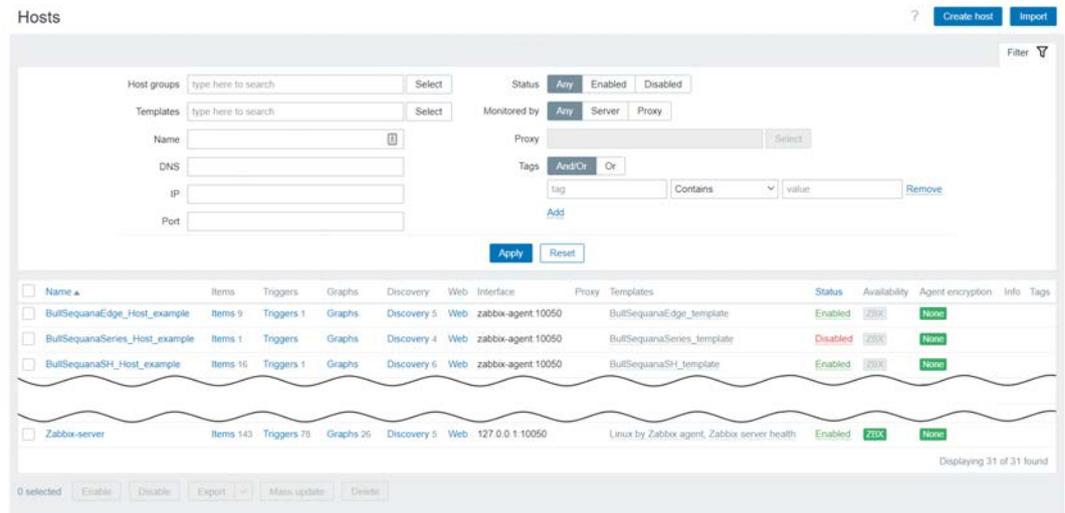
Macro	Value
{MODNUMBER}	Host module number
{OPENBMC}	Host OpenBMC address
{PASSWORD}	Host OpenBMC password
{PORT}	Host OpenBMC port
{USER}	Host OpenBMC username

7. Click **Update**.

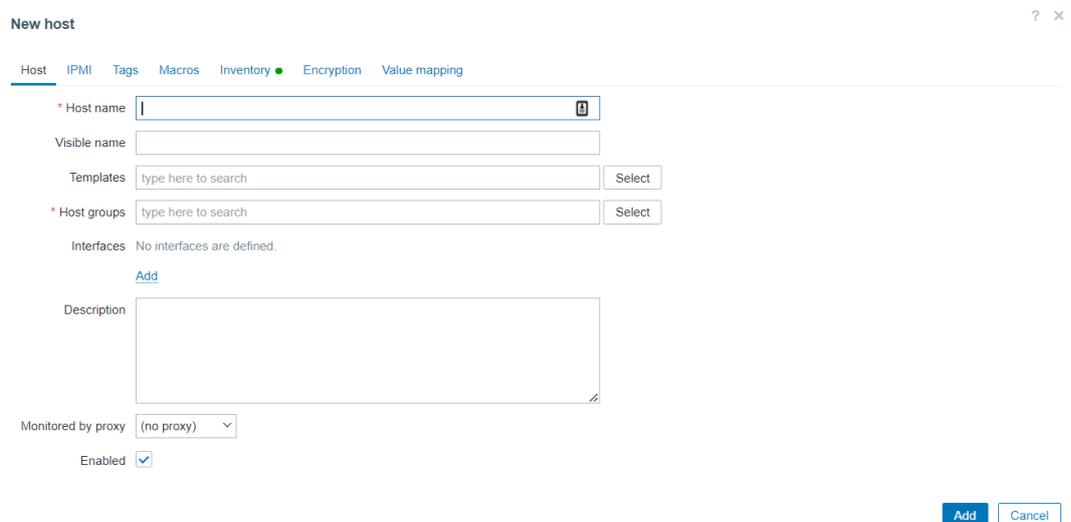
4.3. Adding a host manually

4.3.1. Creating a host

1. From the **Data collection** menu, click the **Hosts** tab. The **Hosts** page opens.



2. On the right-hand side of the screen, click **Create host**. The **New host** page opens.



3. Complete the **Host name** field with the host BMC IP address.

Note The host name may contain alphanumeric characters, spaces, dots, dashes and underscores. Leading and trailing spaces are not allowed.

4. In the **Host groups** section, click **Select** and select **Zabbix servers**.
5. In the **Interfaces** section, perform the following actions:
 - a. click **Add**.
 - b. Select **Agent** in the list.

A new Agent line is created.

The screenshot shows the 'New host' configuration page. The 'Interfaces' section is highlighted with a red box. It contains a table with the following data:

Type	IP address	DNS name	Connect to	Port	Default
Agent	127.0.0.1		IP DNS	10050	Remove

Below the table, there is an 'Add' button and a 'Cancel' button.

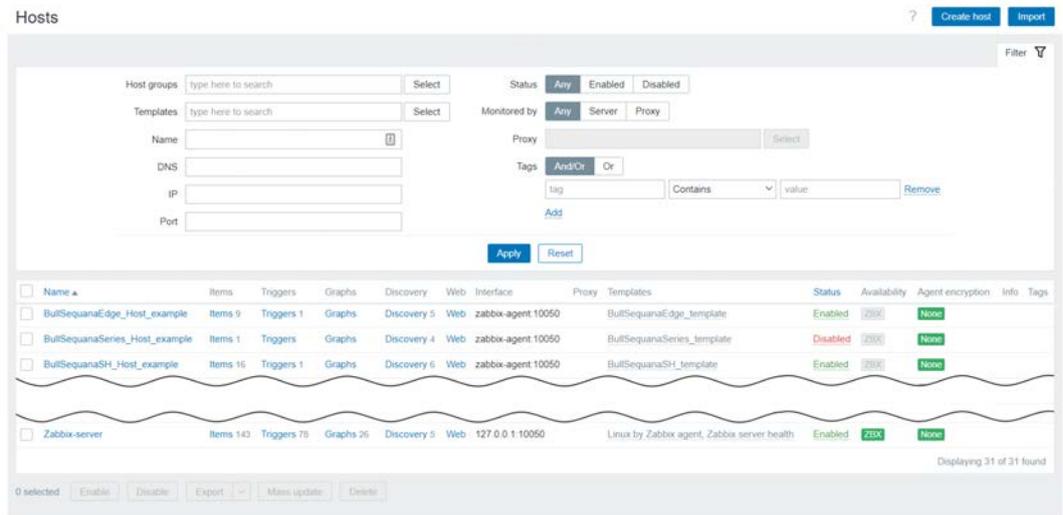
- c. Click **DNS**.
- d. Complete the following fields:

Field	Value
IP address	Clear this field and leave it empty.
DNS name	zabbix-agent
Port	10050

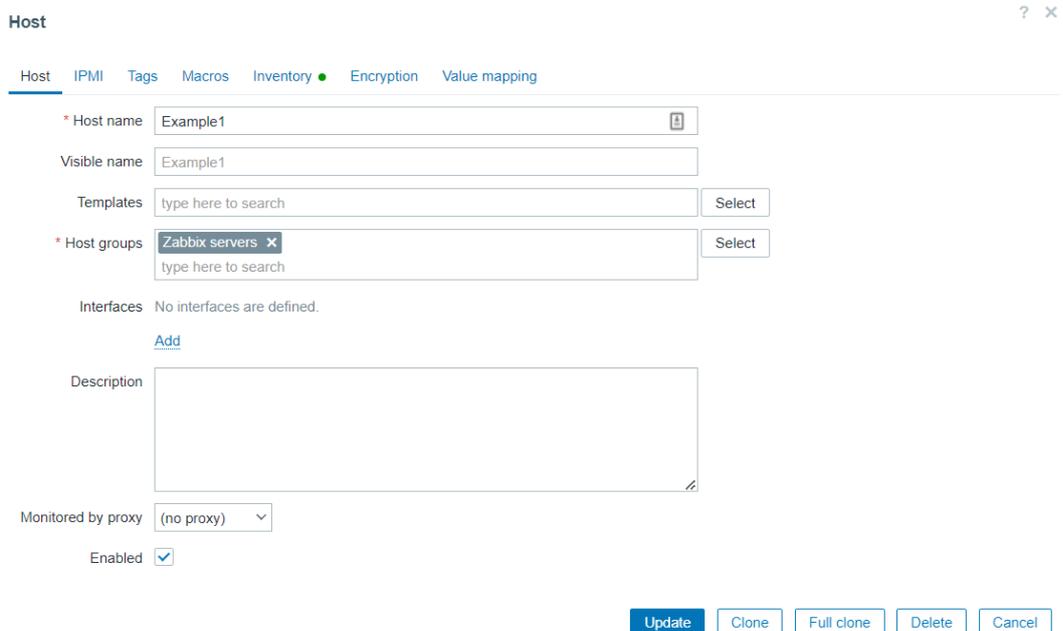
6. Click **Add**.

4.3.2. Linking a host to the template

1. From the **Data collection** menu, click the **Hosts** tab. The **Hosts** page opens.



2. Select a host name. A new page opens.



3. In the **Templates** section, click **Select**. The **Template** page opens.

Templates ×

Template group Select

<input type="checkbox"/>	Brocade FC by SNMP
<input type="checkbox"/>	Brocade_Foundry Nonstackable by SNMP
<input type="checkbox"/>	Brocade_Foundry Stackable by SNMP
<input type="checkbox"/>	BullSequanaEdge_template
<input type="checkbox"/>	BullSequanaSeries_template
<input checked="" type="checkbox"/>	BullSequanaSH_template
<input type="checkbox"/>	Ceph by Zabbix agent 2
<input type="checkbox"/>	Chassis by IPMI
<input type="checkbox"/>	Cisco ASAv by SNMP
<input type="checkbox"/>	Cisco Catalyst 3750V2-24FS by SNMP
<input type="checkbox"/>	Cisco Catalyst 3750V2-24PS by SNMP
<input type="checkbox"/>	Cisco Catalyst 3750V2-24TS by SNMP
<input type="checkbox"/>	Cisco Catalyst 3750V2-48PS by SNMP
<input type="checkbox"/>	Cisco Catalyst 3750V2-48TS by SNMP
<input type="checkbox"/>	Cisco IOS by SNMP
<input type="checkbox"/>	Cisco IOS prior to 12.0_3_T by SNMP

Select Cancel

4. Select the <server_model>_ template.

5. Click **Select**.

The template is displayed in the **Templates** field.

The screenshot shows the 'Host' configuration page in MONGUI. The page has a header with the title 'Host' and a close button. Below the header is a navigation bar with tabs: Host, IPMI, Tags, Macros, Inventory (selected), Encryption, and Value mapping. The main content area contains several fields:

- * Host name:** A text input field containing 'Example1'.
- Visible name:** A text input field containing 'Example1'.
- Templates:** A dropdown menu showing 'BullSequanaSH_template' with a close button and a 'Select' button. Below the dropdown is a search input field with the placeholder 'type here to search'.
- * Host groups:** A dropdown menu showing 'Zabbix servers' with a close button and a 'Select' button. Below the dropdown is a search input field with the placeholder 'type here to search'.
- Interfaces:** A section with the text 'No interfaces are defined.' and an 'Add' link.
- Description:** A large text area for entering a description.
- Monitored by proxy:** A dropdown menu currently set to '(no proxy)'.
- Enabled:** A checkbox that is checked.

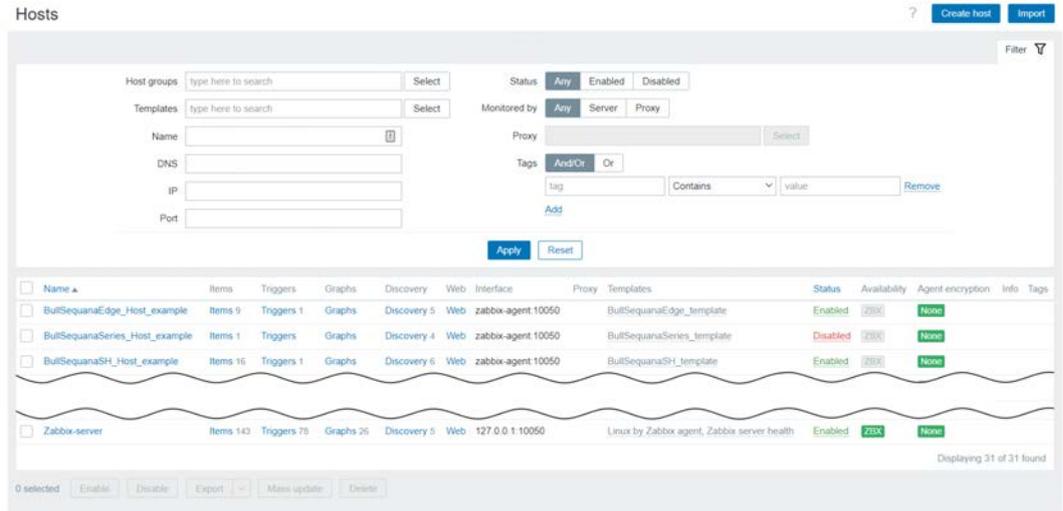
At the bottom right of the form, there are five buttons: 'Update' (highlighted with a red box), 'Clone', 'Full clone', 'Delete', and 'Cancel'.

6. Click **Update**.

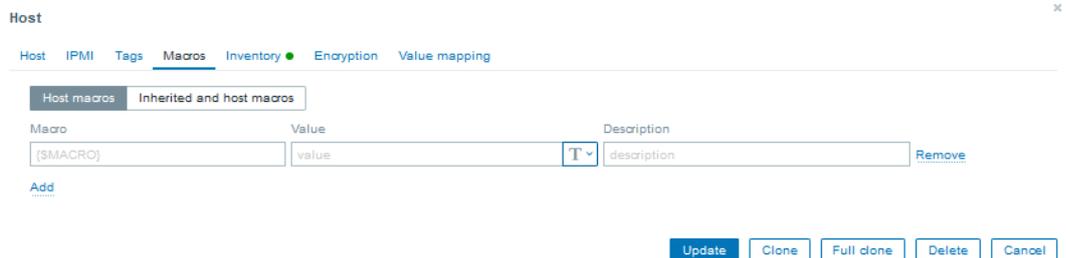
4.3.3. Adding macros on a host

Five macros must be added on a host.

1. From the **Data collection** menu, click the **Hosts** tab. The **Hosts** page opens.



2. Select a host name. A new page opens.
3. Click the **Macros** tab.



4. Add the macros:

Macro	Value
{\$MODNUMBER}	Host module number
{\$OPENBMC}	Host OpenBMC address
{\$PASSWORD}	Host OpenBMC password
{\$PORT}	Host OpenBMC port
{\$USER}	Host OpenBMC username

For each macro:

- Complete the **Macro** and **Value** fields.
- Click **Add**.

Example

Host

Host IPMI Tags Macros 5 Inventory Encryption Value mapping

Host macros Inherited and host macros

Macro	Value	Description
{\$MODNUMBER}	0	description
{\$OPENBMC}	XX.XX.XX.XX	description
{\$PASSWORD}	my@password	description
{\$PORT}	443	description
{\$USER}	root	description

Add

Update Clone Full clone Delete Cancel

5. Click **Update**

Chapter 5. Monitoring rsyslog

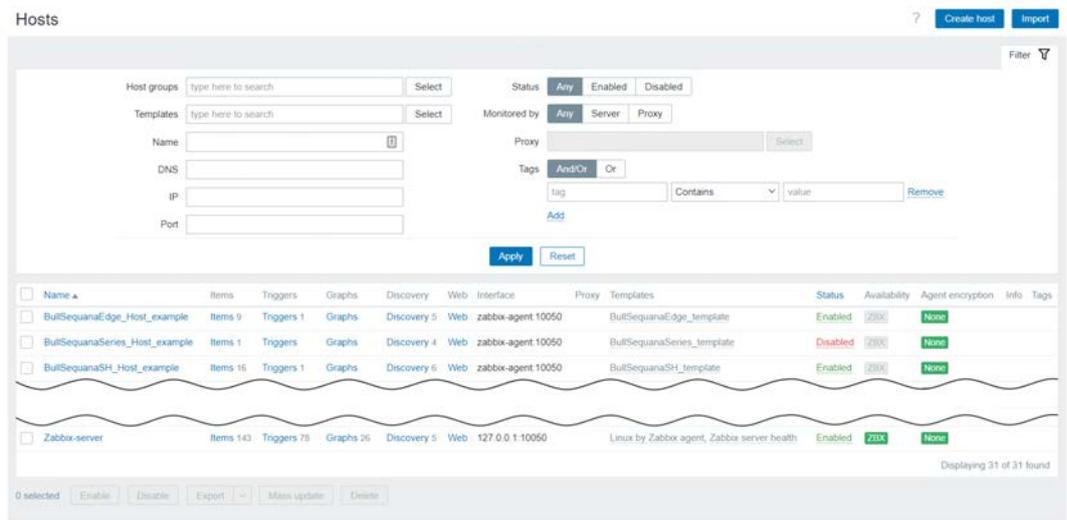
Zabbix can be used to analyze the log files of a host.

Prerequisites

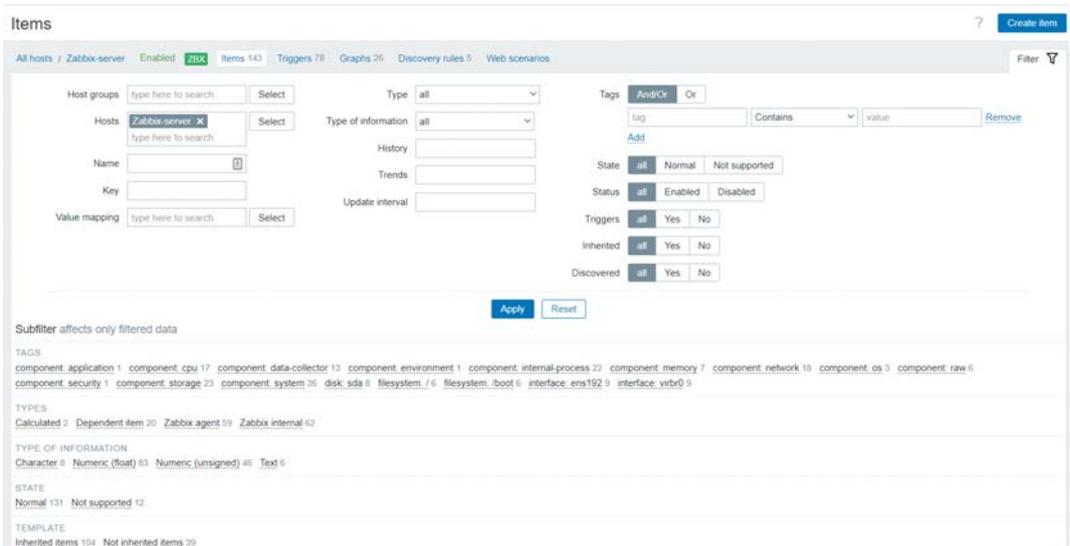
- The Zabbix agent is running on the host
- The Log monitoring item is set up for the host

Procedure

1. From the **Data collection** menu, click the **Hosts** tab. The **Hosts** page opens.



2. Click **Items** of the Zabbix-server line. The **Items** page opens.



3. Click **Create item** and complete the required fields.

Items

All hosts / Zabbix server Enabled ZBX Items 137 Triggers 73 Graphs 26 Discovery rules 4 Web scenarios

Item Tags Preprocessing

* Name

Type

* Key

Type of information

* Host interface

* Update interval

Custom intervals

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

* History storage period

Log time format

Description

Enabled

4. Click **Add**.

5. Enable rsyslog on the Zabbix server side.

- a. In `/etc/rsyslog.conf` file, uncomment or copy the following lines:

```
# Provides UDP syslog reception
# for parameters see http://www.rsyslog.com/doc/imudp.html
module(load="imudp") # needs to be done just once
input(type="imudp" port="514")

# Provides TCP syslog reception
# for parameters see http://www.rsyslog.com/doc/imtcp.html
module(load="imtcp") # needs to be done just once
input(type="imtcp" port="514")
```

- b. Check the firewall configuration, the rsyslog default port 514 must be open for tcp and udp protocols.
- c. Create your own rsyslog configuration file in `/etc/rsyslog.d` directory.

```
$template rsyslog_format54,"[<font color=red>%FROMHOST-IP%</font>]
%timegenerated% %hostname% %syslogfacility-text%:%syslogpriority-text%
%syslogtag%:msg:::drop-last-lf%n"
$template RemoteBmcLogs54,"/var/log/rsyslog/zabbix54.log"
:FROMHOST-IP, isequal, "10.xx.xx.54" ?RemoteBmcLogs54;rsyslog_format54
& ~
```

- d. Restart the rsyslog service.

```
systemctl restart rsyslog.service
```

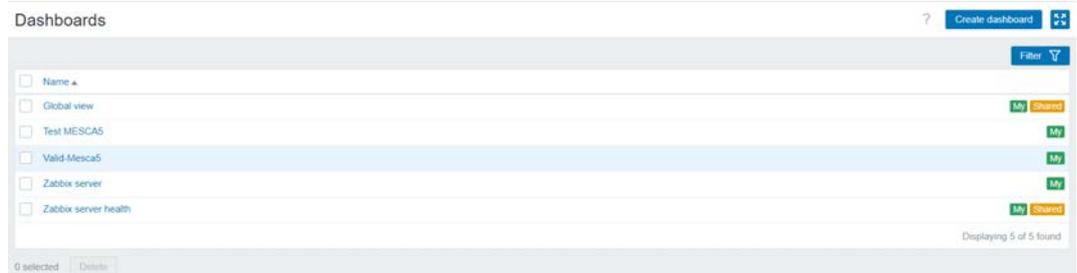
- e. Connect to the management controller of the host and check that the connection is logged in the rsyslog previously created.

```
[root@frcla009-vm rsyslog]# pwd /var/log/rsyslog
[root@frcla009-vm rsyslog]# more zabbix54.log
[<font color=red>10.xx.xx.54</font>] Jun 12 15:55:10 User user:info
'super' from host '10.xx.xx.xxx' logged in.
...
```

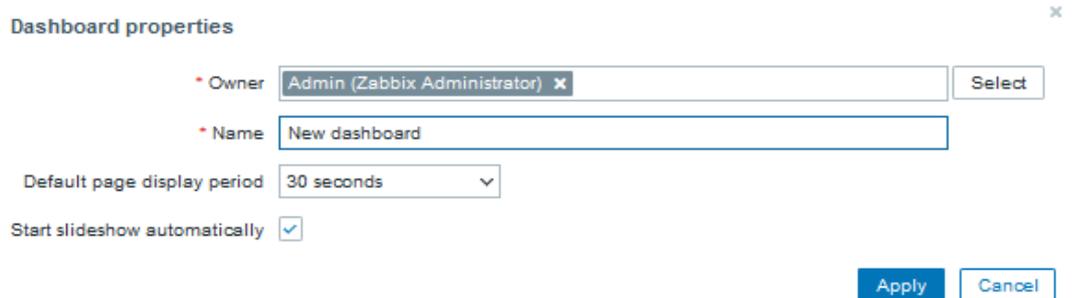
Chapter 6. Customizing the Zabbix console

6.1. Creating a dashboard

1. Click **Dashboard** in the menu. The **Dashboards** page opens.



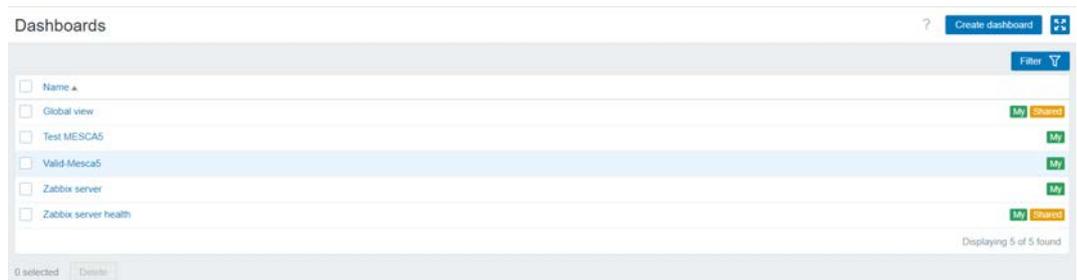
2. On the right-hand side of the screen, click **Create dashboard**. A **Dashboard properties** pop-up window opens.
3. In the **Owner** field, click **Select**.
4. Select an owner.

A screenshot of the "Dashboard properties" pop-up window. The window title is "Dashboard properties" and it has a close button (X) in the top right corner. The form contains the following fields: "Owner" (a dropdown menu showing "Admin (Zabbix Administrator)" with a "Select" button to its right), "Name" (a text input field containing "New dashboard"), "Default page display period" (a dropdown menu showing "30 seconds"), and "Start slideshow automatically" (a checked checkbox). At the bottom right of the form are "Apply" and "Cancel" buttons.

5. Complete the fields as required.
6. Click **Apply**.
7. Click **Save changes**.

6.2. Adding a graph to a dashboard

1. Click **Dashboard** in the menu. The **Dashboards** page opens.

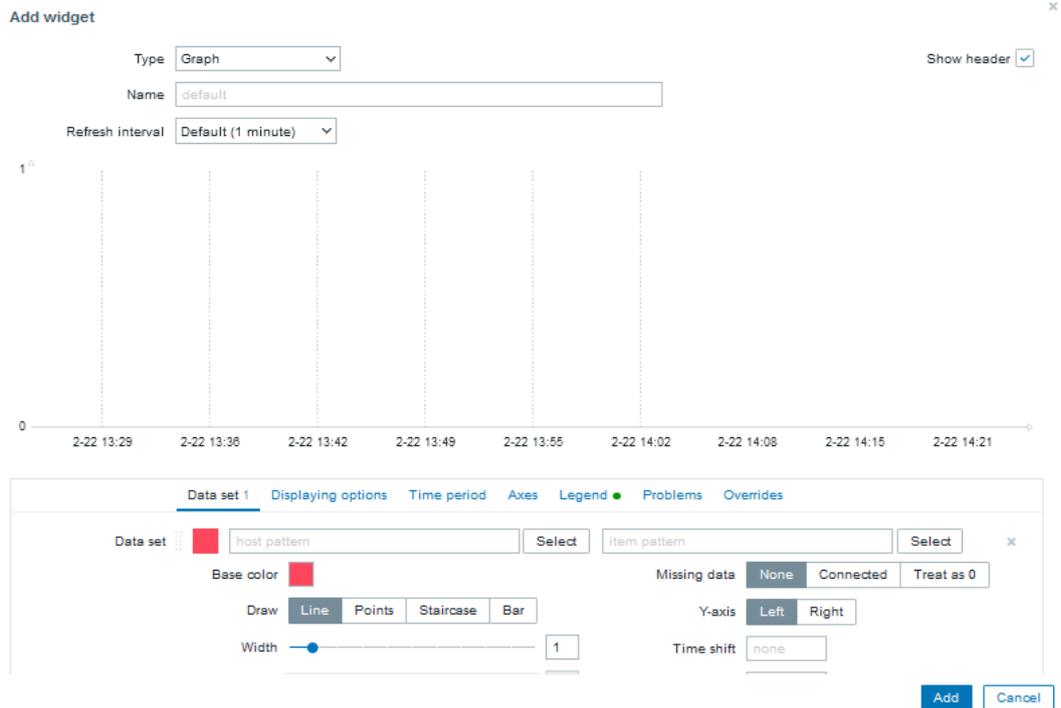


2. Select a dashboard. A new page opens.



3. Click **Edit dashboard**.
4. Click **Add widget** in **Add** drop-down menu. The **Add widget** pop-up window opens.

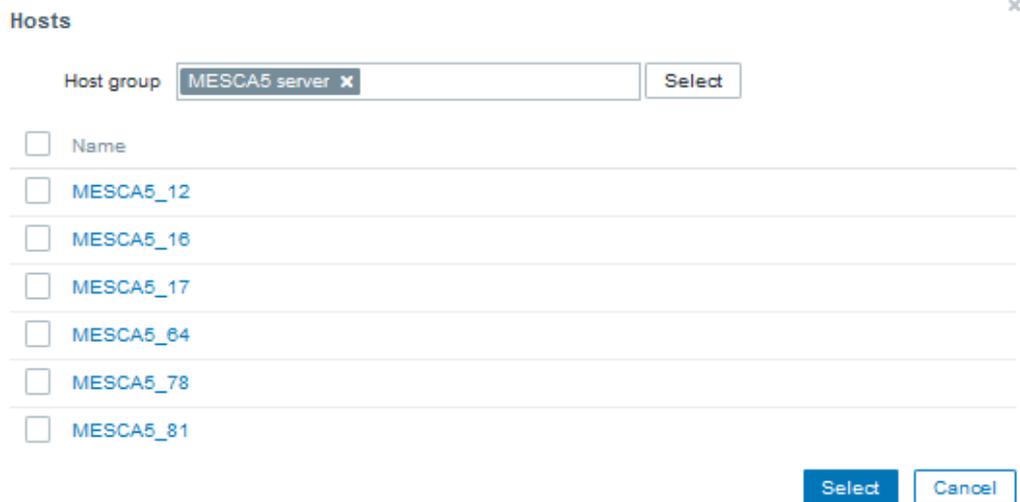
5. From the **Type** drop-down list, select **Graph**.



6. Click the **Data set** tab.

7. Select the hosts to compare.

a. In the **host pattern** field, click Select. A new page opens.



b. Select the required hosts.

c. Click **Select**.

8. Select the item to display.
 - a. In the **item pattern** field, click **Select**. A new page opens.

Items

Host:

<input type="checkbox"/>	Name	Key	Type	Type of information	Status
<input type="checkbox"/>	CPU0_Inlet_Temp LowerThresholdCritical	mesca5_openbmc_sensors_reader[-f=\${SOPENBMC}-Module\${MODNUMBER}-Thermal.json,-g=Temperatures,-i=CPU0_Inlet_Temp,-p=LowerThresholdCritical]	External check	Numeric (float)	Enabled
<input type="checkbox"/>	CPU0_Inlet_Temp LowerThresholdNonCritical	mesca5_openbmc_sensors_reader[-f=\${SOPENBMC}-Module\${MODNUMBER}-Thermal.json,-g=Temperatures,-i=CPU0_Inlet_Temp,-p=LowerThresholdNonCritical]	External check	Numeric (float)	Enabled
<input type="checkbox"/>	CPU0_Inlet_Temp Reading	mesca5_openbmc_sensors_reader[-f=\${SOPENBMC}-Module\${MODNUMBER}-Thermal.json,-g=Temperatures,-i=CPU0_Inlet_Temp,-p=ReadingCelsius]	External check	Numeric (float)	Enabled
<input type="checkbox"/>	CPU0_Inlet_Temp UpperThresholdCritical	mesca5_openbmc_sensors_reader[-f=\${SOPENBMC}-Module\${MODNUMBER}-Thermal.json,-g=Temperatures,-i=CPU0_Inlet_Temp,-p=UpperThresholdCritical]	External check	Numeric (float)	Enabled
<input type="checkbox"/>	CPU0_Inlet_Temp UpperThresholdNonCritical	mesca5_openbmc_sensors_reader[-f=\${SOPENBMC}-Module\${MODNUMBER}-Thermal.json,-g=Temperatures,-i=CPU0_Inlet_Temp,-p=UpperThresholdNonCritical]	External check	Numeric (float)	Enabled
<input type="checkbox"/>	CPU1_Inlet_Temp LowerThresholdCritical	mesca5_openbmc_sensors_reader[-f=\${SOPENBMC}-Module\${MODNUMBER}-Thermal.json,-g=Temperatures,-i=CPU1_Inlet_Temp,-p=LowerThresholdCritical]	External check	Numeric (float)	Enabled
<input type="checkbox"/>	CPU1_Inlet_Temp LowerThresholdNonCritical	mesca5_openbmc_sensors_reader[-f=\${SOPENBMC}-Module\${MODNUMBER}-Thermal.json,-g=Temperatures,-i=CPU1_Inlet_Temp,-p=LowerThresholdNonCritical]	External check	Numeric (float)	Enabled
<input type="checkbox"/>	CPU1_Inlet_Temp Reading	mesca5_openbmc_sensors_reader[-f=\${SOPENBMC}-Module\${MODNUMBER}-Thermal.json,-g=Temperatures,-i=CPU1_Inlet_Temp,-p=ReadingCelsius]	External check	Numeric (float)	Enabled
<input type="checkbox"/>	CPU1_Inlet_Temp UpperThresholdCritical	mesca5_openbmc_sensors_reader[-f=\${SOPENBMC}-Module\${MODNUMBER}-Thermal.json,-g=Temperatures,-i=CPU1_Inlet_Temp,-p=UpperThresholdCritical]	External check	Numeric (float)	Enabled
<input type="checkbox"/>	CPU1_Inlet_Temp UpperThresholdNonCritical	mesca5_openbmc_sensors_reader[-f=\${SOPENBMC}-Module\${MODNUMBER}-Thermal.json,-g=Temperatures,-i=CPU1_Inlet_Temp,-p=UpperThresholdNonCritical]	External check	Numeric (float)	Enabled

- b. Select the required items.
 - c. Click **Select**.
9. From the **Add widget** page, complete the fields as required.
10. Click **Add**. The selected graph is added to the dashboard.

Dashboard_example Edit dashboard

Dashboard updated

All dashboards / Dashboard_example

From: 2023-02-22 11:47:09 To: 2023-02-22 12:47:09

Zoom out

2023-02-22 11:47:09 – 2023-02-22 12:47:09

Last 2 days	Yesterday	Today	Last 5 minutes
Last 7 days	Day before yesterday	Today so far	Last 15 minutes
Last 30 days	This day last week	This week	Last 30 minutes
Last 3 months	Previous week	This week so far	Last 1 hour
Last 6 months	Previous month	This month	Last 3 hours
Last 1 year	Previous year	This month so far	Last 6 hours
Last 2 years		This year	Last 12 hours
		This year so far	Last 1 day

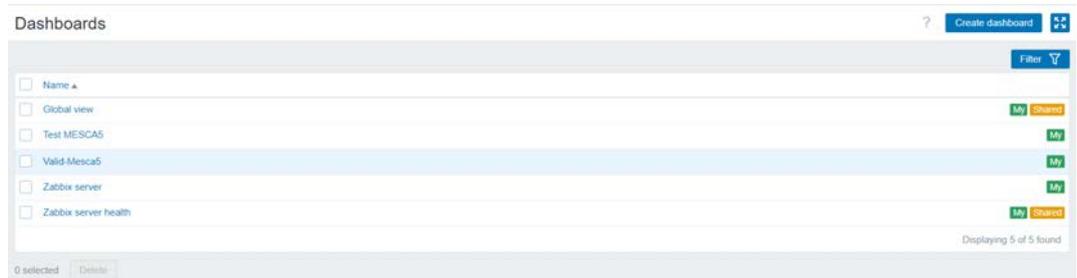
Graph

MESCA5_12: CPU0_Inlet_Temp UpperThresholdCritical

11. Click **Save changes**.

6.3. Adding a predefined graph prototype to a dashboard

1. Click **Dashboard** in the menu. The **Dashboards** page opens.



2. Select a dashboard. A new page opens.



3. Click **Edit dashboard**.
4. Click **Add widget** in **Add** drop-down menu. The **Add widget** pop-up window opens.

- From the **Type** drop-down list, select **Graph prototype**.
- In the **Source** field, select **Graph prototype**.

Add widget x

Type Show header

Name

Refresh interval

Source

* Graph prototype

Show legend

Dynamic item

* Columns

* Rows

- In the **Graph prototype** field, click **Select**. The **Graph prototypes** window opens.

Graph prototypes x

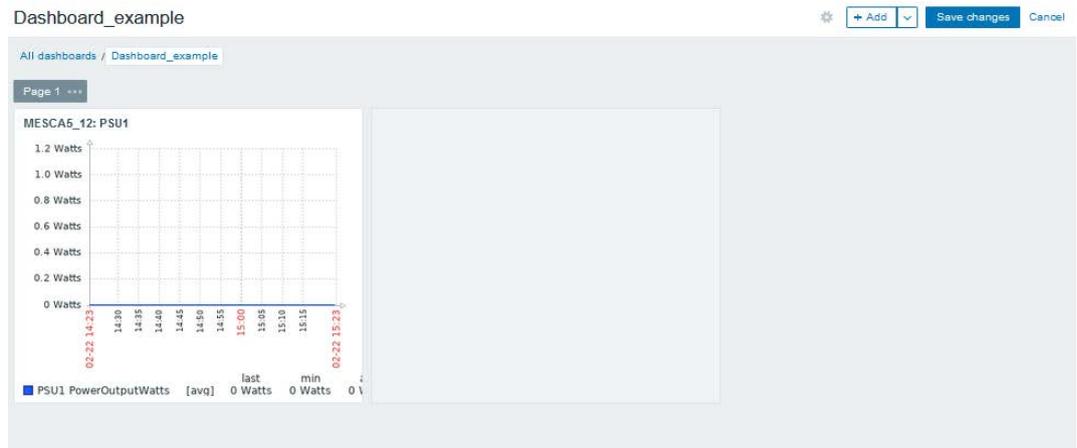
Host

Name	Graph type
{#FAN}	Normal
{#POWERSUPPLIE}	Normal
{#TEMPERATURE}	Normal
{#VOLTAGE}	Normal

- Select the required graph prototype.
- From the **Add widget** page, complete the **Columns** and **Rows** fields as required.

10. Click **Add**.

The selected graph prototype is added to the dashboard.

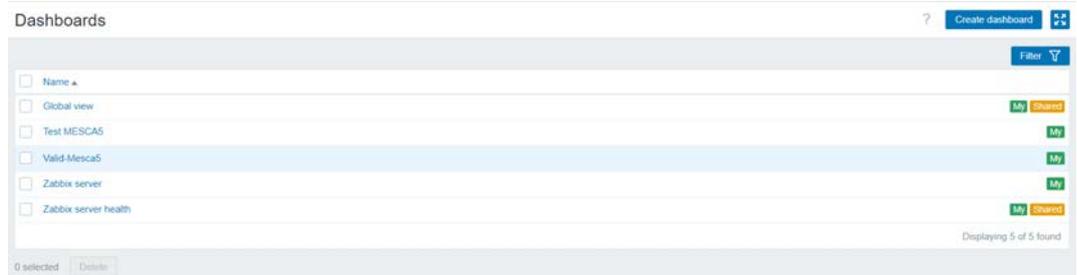


11. Click **Save changes**.

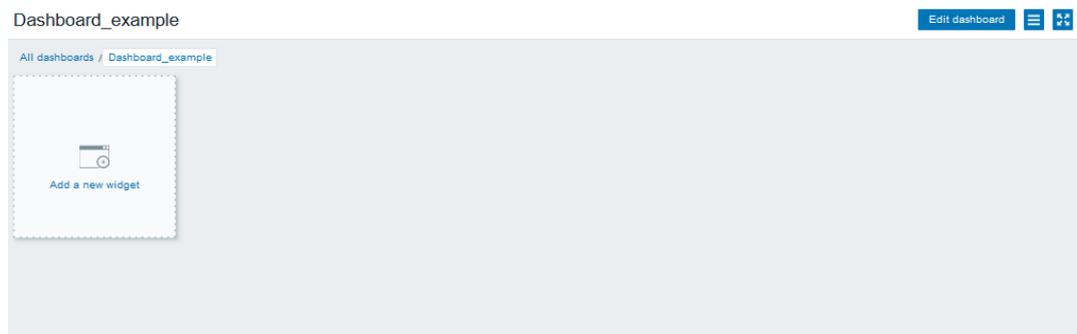
6.4. Adding a plain text to a dashboard

Note When it has been enabled, rsyslog is a type of plain text.

1. Click **Dashboard** in the menu. The **Dashboards** page opens.



2. Select a dashboard. A new page opens.



3. Click **Edit dashboard**.
4. Click **Add widget** in **Add** drop-down menu. The **Add widget** pop-up window opens.

- From the **Type** drop-down list, select **Plain text**.

Add widget ✕

Type: Plain text Show header

Name:

Refresh interval: Default (1 minute)

* Items: Select

Items location: Left Top

* Show lines:

Show text as HTML:

Dynamic items:

Add Cancel

- In the **Show lines** field, enter the number of lines to display.
- In the **Items** field, click **Select**. The **Items** pop-up window opens.

Items ✕

Host: MESCA5_12 Select

<input type="checkbox"/>	Name	Key	Type	Type of information	Status
<input type="checkbox"/>	BIOS_state	mesca5_openbmc_fw_reader[-f={SOPENBMC}-Module{MODNUMBER}-firmwares.json,-i=BIOS,-p=Status,-s=State]	External check	Text	Enabled
<input type="checkbox"/>	BIOS_version	mesca5_openbmc_fw_reader[-f={SOPENBMC}-Module{MODNUMBER}-firmwares.json,-i=BIOS,-p=Version]	External check	Text	Enabled
<input type="checkbox"/>	BMC_state	mesca5_openbmc_fw_reader[-f={SOPENBMC}-Module{MODNUMBER}-firmwares.json,-i=BMC,-p=Status,-s=State]	External check	Text	Enabled
<input type="checkbox"/>	BMC_version	mesca5_openbmc_fw_reader[-f={SOPENBMC}-Module{MODNUMBER}-firmwares.json,-i=BMC,-p=Version]	External check	Text	Enabled
<input type="checkbox"/>	CEB_IO_FPGA_version	mesca5_openbmc_fw_reader[-f={SOPENBMC}-Module{MODNUMBER}-firmwares.json,-i=CEB_IO_FPGA,-p=Version]	External check	Text	Enabled
<input type="checkbox"/>	CEB_MAIN_FPGA_version	mesca5_openbmc_fw_reader[-f={SOPENBMC}-Module{MODNUMBER}-firmwares.json,-i=CEB_MAIN_FPGA,-p=Version]	External check	Text	Enabled
<input type="checkbox"/>	CEB_P_CPLD_version	mesca5_openbmc_fw_reader[-f={SOPENBMC}-Module{MODNUMBER}-firmwares.json,-i=CEB_P_CPLD,-p=Version]	External check	Text	Enabled
<input type="checkbox"/>	CPU0_Inlet_Temp LowerThresholdCritical	mesca5_openbmc_sensors_reader[-f={SOPENBMC}-Module{MODNUMBER}-Thermal.json,-g=Temperatures,-i=CPU0_Inlet_Temp,-p=LowerThresholdCritical]	External check	Numeric (float)	Enabled
<input type="checkbox"/>	CPU0_Inlet_Temp LowerThresholdNonCritical	mesca5_openbmc_sensors_reader[-f={SOPENBMC}-Module{MODNUMBER}-Thermal.json,-g=Temperatures,-i=CPU0_Inlet_Temp,-p=LowerThresholdNonCritical]	External check	Numeric (float)	Enabled
<input type="checkbox"/>	CPU0_Inlet_Temp Reading	mesca5_openbmc_sensors_reader[-f={SOPENBMC}-Module{MODNUMBER}-Thermal.json,-g=Temperatures,-i=CPU0_Inlet_Temp,-p=ReadingCelsius]	External check	Numeric (float)	Enabled
<input type="checkbox"/>	CPU0_Inlet_Temp UpperThresholdCritical	mesca5_openbmc_sensors_reader[-f={SOPENBMC}-Module{MODNUMBER}-Thermal.json,-g=Temperatures,-i=CPU0_Inlet_Temp,-p=UpperThresholdCritical]	External check	Numeric (float)	Enabled

Select Cancel

- Select the required items.
- Click **Select**.

- From the **Add widget** page, complete the fields as required.

Add widget ✕

Type Show header

Name

Refresh interval

* Items Select

Items location

* Show lines

Show text as HTML

Dynamic items

- Click **Add**.

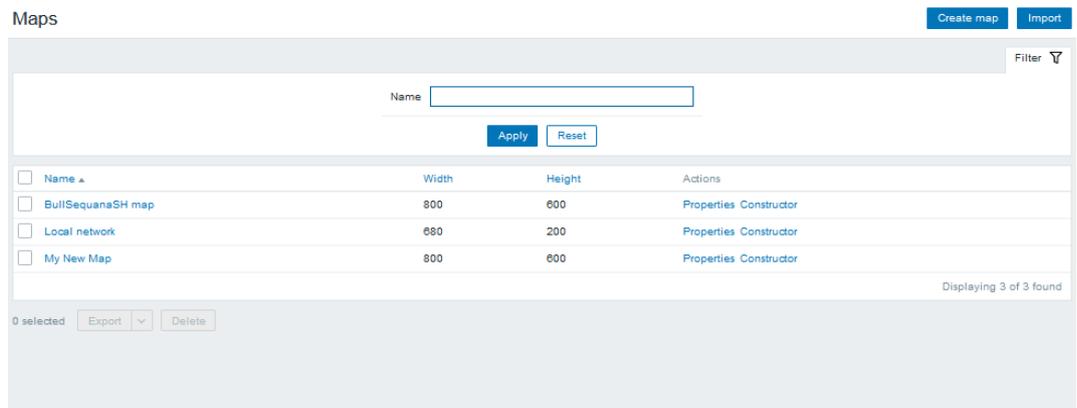
The plain text is added to the dashboard.



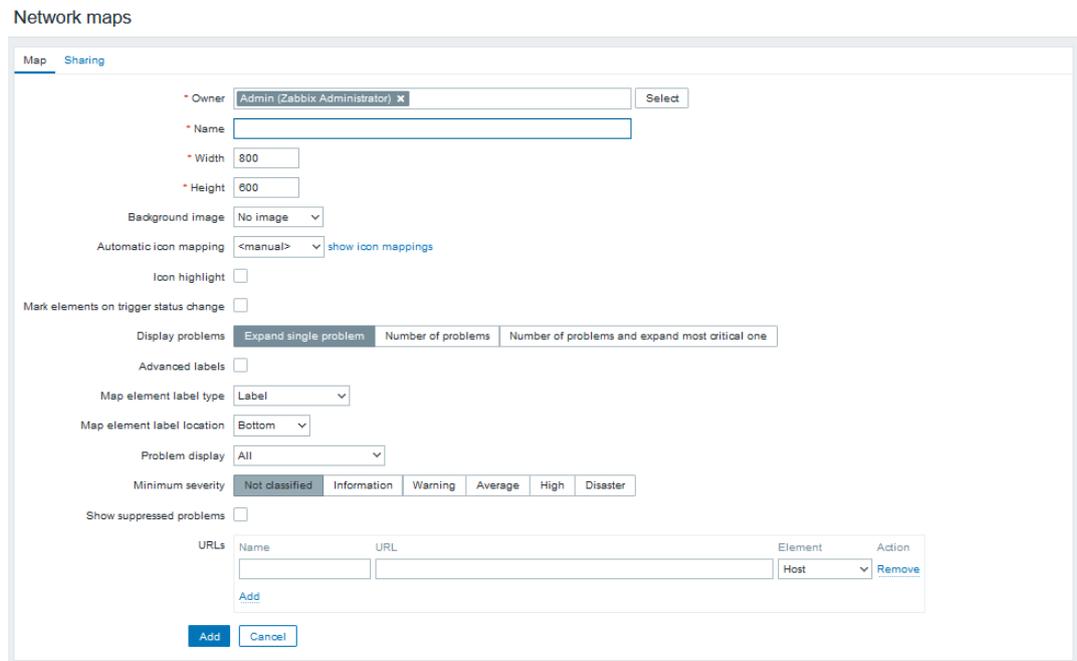
- From the **Dashboard** page, click **Save changes**.

6.5. Adding a map

1. From the **Monitoring** menu, click **Maps**. The **Maps** page opens.



2. On the right-hand side of the screen, click **Create Map**. The **Network maps** page opens.



3. Enter a name in the **Name** field.
4. Select the **Icon highlight** and **Mark elements on trigger status change** check boxes.

5. Complete the fields as required.

Network maps

The screenshot shows the 'Network maps' configuration form. The 'Owner' field is set to 'Admin (Zabbix Administrator)'. The 'Name' field is 'Map_example'. The 'Width' is 800 and 'Height' is 600. The 'Background image' is 'No image'. The 'Automatic icon mapping' is '<manual>'. The 'Icon highlight' and 'Mark elements on trigger status change' checkboxes are checked. The 'Display problems' tabs are 'Expand single problem', 'Number of problems', and 'Number of problems and expand most critical one'. The 'Advanced labels' checkbox is unchecked. The 'Map element label type' is 'Label', 'Map element label location' is 'Bottom', and 'Problem display' is 'All'. The 'Minimum severity' tabs are 'Not classified', 'Information', 'Warning', 'Average', 'High', and 'Disaster'. The 'Show suppressed problems' checkbox is unchecked. The 'URLs' table has one row with 'Name', 'URL', 'Element', and 'Action' columns. The 'Element' is 'Host' and the 'Action' is 'Remove'. There are 'Add' and 'Cancel' buttons at the bottom.

6. Click **Add**.

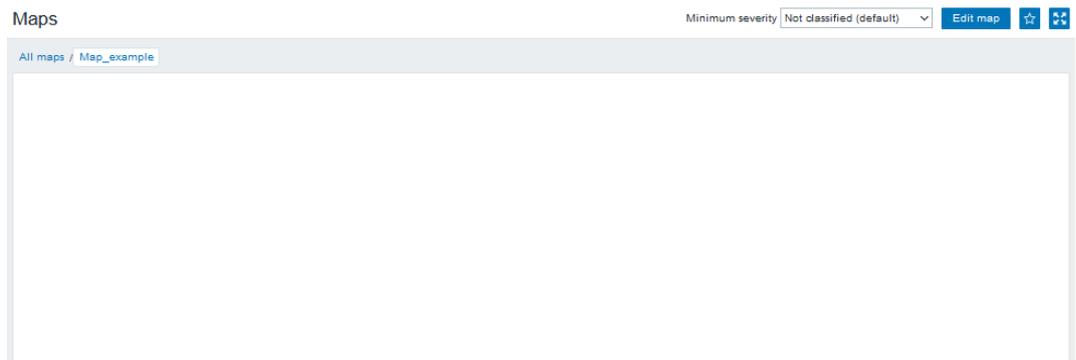
The new map is created.

The screenshot shows the 'Maps' page. At the top right, there are 'Create map' and 'Import' buttons. A confirmation message 'Network map added' is displayed. Below the message is a search bar with a 'Filter' icon. The main content is a table of maps:

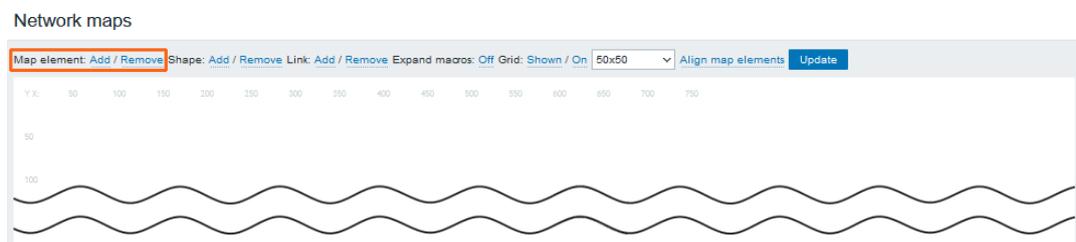
<input type="checkbox"/>	Name	Width	Height	Actions
<input type="checkbox"/>	BullSequanaSH map	800	600	Properties Constructor
<input type="checkbox"/>	Local network	680	200	Properties Constructor
<input type="checkbox"/>	Map_example	800	600	Properties Constructor
<input type="checkbox"/>	My New Map	800	600	Properties Constructor

At the bottom, it says '0 selected' and 'Export' and 'Delete' buttons. The text 'Displaying 4 of 4 found' is at the bottom right.

- From the **Maps** page, select the new map. The **Maps** page opens.

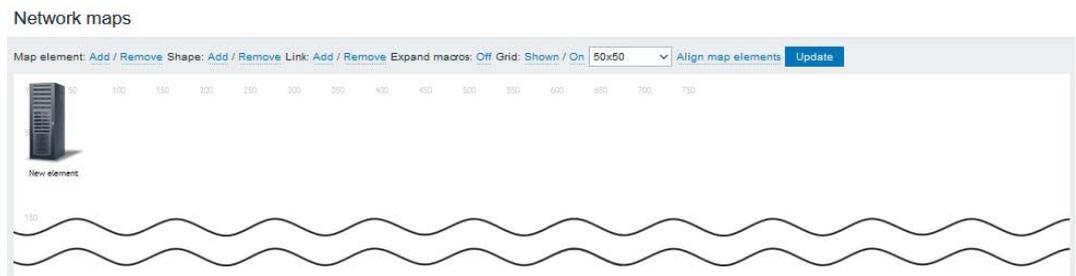


- Click **Edit map**. The **Network maps** page opens.



- From the **Map element** section, click **Add**.

A new element appears.



10. Click on the new element. The **Map element** pop-up window opens.

Map element

Type

Label

Label location

Icons

Coordinates X Y

Name	URL	Action
<input type="text"/>	<input type="text"/>	Remove

[Add](#)

11. From the **Type** drop-down list, select **Host**.

12. Enter a label in the **Label** field.

13. In the **Host** field, click **Select**.

14. Select the required host.

Hosts ✕

Host group

Name

MESCA5_12
MESCA5_16
MESCA5_17
MESCA5_64
MESCA5_78
MESCA5_81

15. In the **Icons** section, from the **Default** drop-down list, select the required icon.

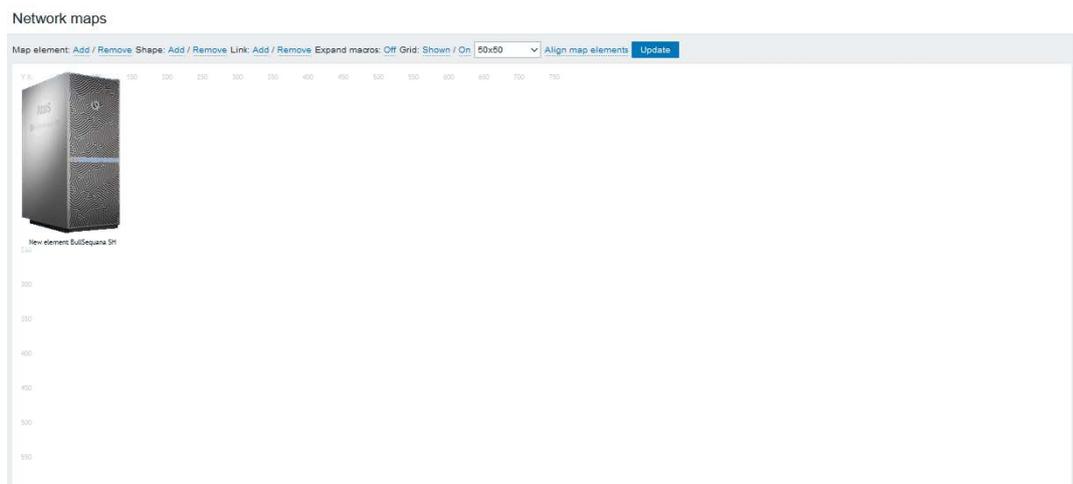
The screenshot shows the 'Map element' configuration form in the Zabbix console. The form is organized into several sections:

- Map element:** Contains a 'Type' dropdown set to 'Host', a 'Label' text input with 'New element BullSequana SH', and a 'Label location' dropdown set to 'Default'.
- *Host:** A text input containing 'MESCA5_12' and a 'Select' button.
- Tags:** Includes radio buttons for 'And/Or' and 'Or', a 'tag' input, a 'Contains' dropdown, a 'value' input, and 'Add' and 'Remove' buttons.
- Automatic icon selection:** A checkbox that is currently unchecked.
- Icons:** A section with four dropdown menus: 'Default' (set to 'BullSequanaSH'), 'Problem' (set to 'Default'), 'Maintenance' (set to 'Default'), and 'Disabled' (set to 'Default').
- Coordinates:** Two input fields for 'X' and 'Y', both set to '0'.
- URLs:** A table with columns for 'Name', 'URL', and 'Action'. It includes 'Add' and 'Remove' buttons.
- Buttons:** 'Apply', 'Remove', and 'Close' buttons at the bottom.

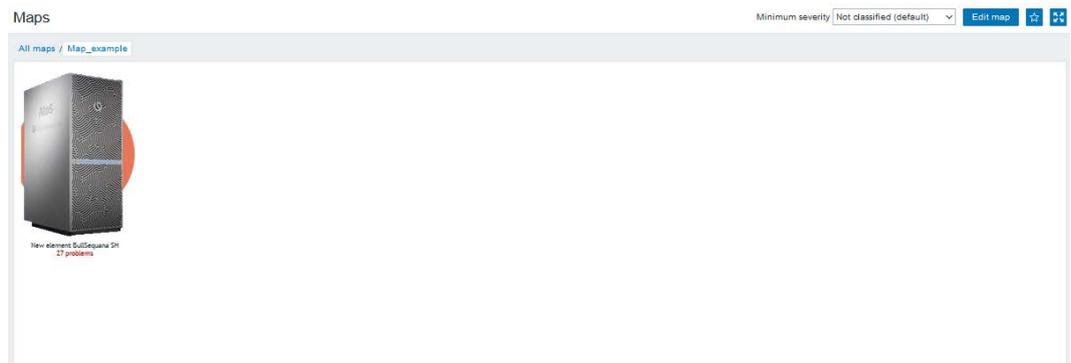
16. Click **Apply**.

17. Click **Close**.

18. From the **Network maps** page, click **Update**.



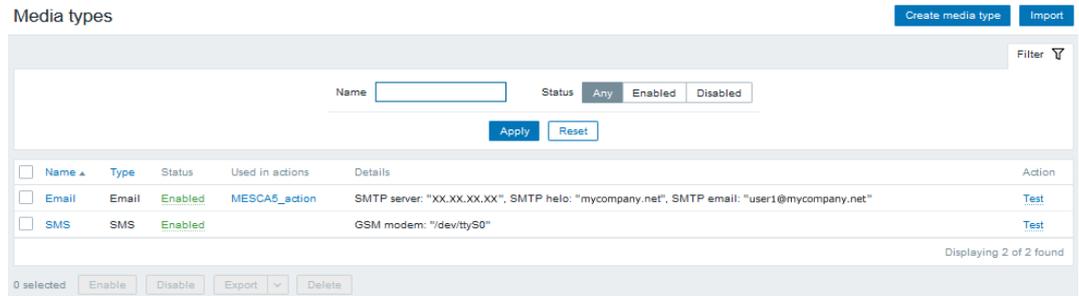
The highest problem severity color and the number of problems are displayed.



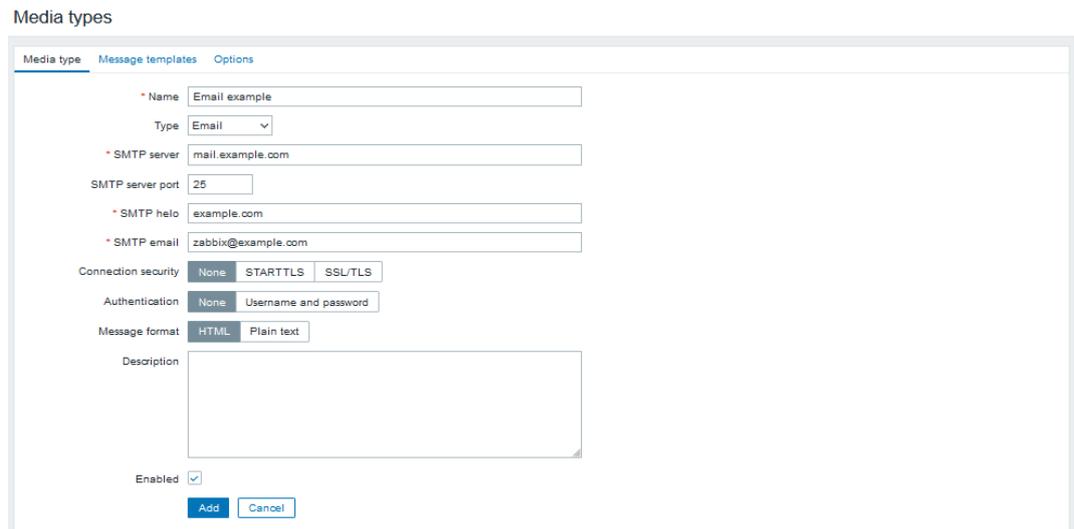
Chapter 7. Setting up emails alerts

7.1. Configuring an email media

1. From the **Alert** menu, click the **Media types** tab. The **Media types** page opens.



2. Click **Create media type**. A new page opens.



3. Complete the **Name** field.
4. Select **Email** from the **Type** drop-down list.
5. Complete the **SMTP server**, **SMTP helo** and **SMTP email** fields as required.

6. Click **Add** to complete changes.

The media type is created.

Example

Media types [Create media type](#) [Import](#)

Media type added x

Name Status Any Enabled Disabled

Apply Reset

<input type="checkbox"/>	Name ▲	Type	Status	Used in actions	Details	Action
<input type="checkbox"/>	Email	Email	Enabled	MESCA5_action	SMTP server: "XX.XX.XX.XX", SMTP helo: "mycompany.net", SMTP email: "user1@mycompany.net"	Test
<input type="checkbox"/>	Email example	Email	Enabled		SMTP server: "mail.example.com", SMTP helo: "example.com", SMTP email: "zabbix@example.com"	Test
<input type="checkbox"/>	SMS	SMS	Enabled		GSM modem: "dev/ttyS0"	Test

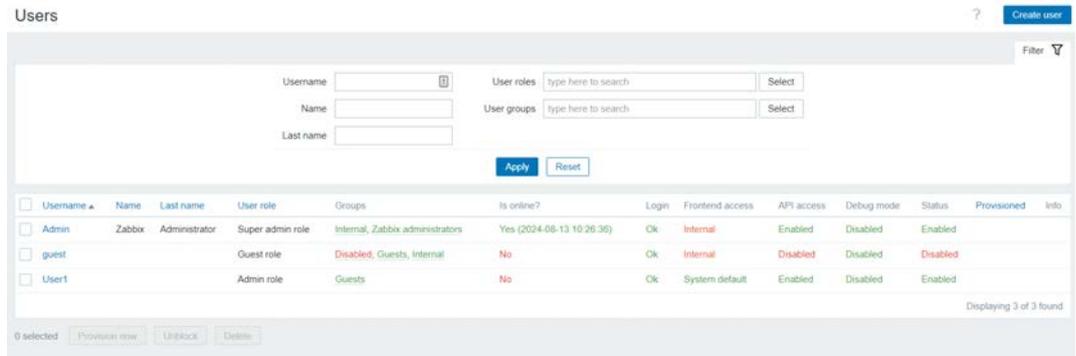
Displaying 3 of 3 found

0 selected Enable Disable Export ▼ Delete

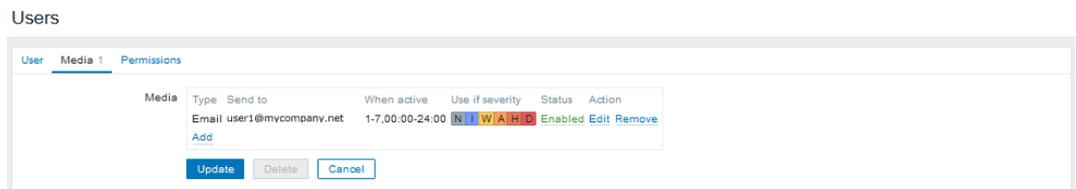
7. Click **Test** to send a test email.

7.2. Adding an email media for a user or a user group

1. From the menu, click the **Users** tab. The **Users** page opens.



2. Select the user required. A new page opens.
3. Click the **Media** tab.



4. In the **Media** section, click **Add**. The **Media** page opens.
 - a. From the **Type** drop-down list, select the media type previously created.
 - b. Complete the fields as required.

Media ✕

Type

* Send to [Remove](#)

[Add](#)

* When active

Use if severity Not classified
 Information
 Warning
 Average
 High
 Disaster

Enabled

- c. Click **Add**.

Example

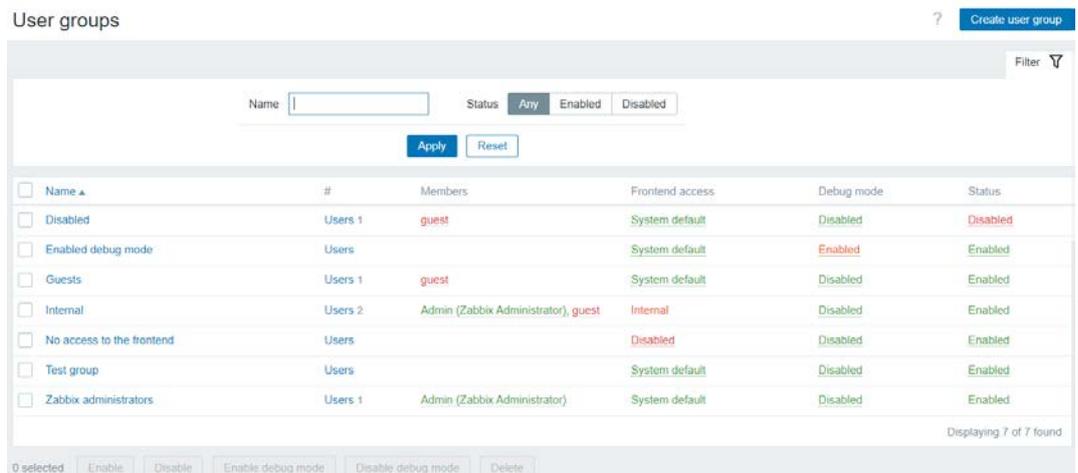
Users

Media						
Type	Send to	When active	Use if severity	Status	Action	
Email	user1@mycompany.net	1-7,00:00-24:00	N I W A R N I N G	Enabled	Edit	Remove
Email example	zabbix@example.com	1-7,00:00-24:00	N I W A R N I N G	Enabled	Edit	Remove

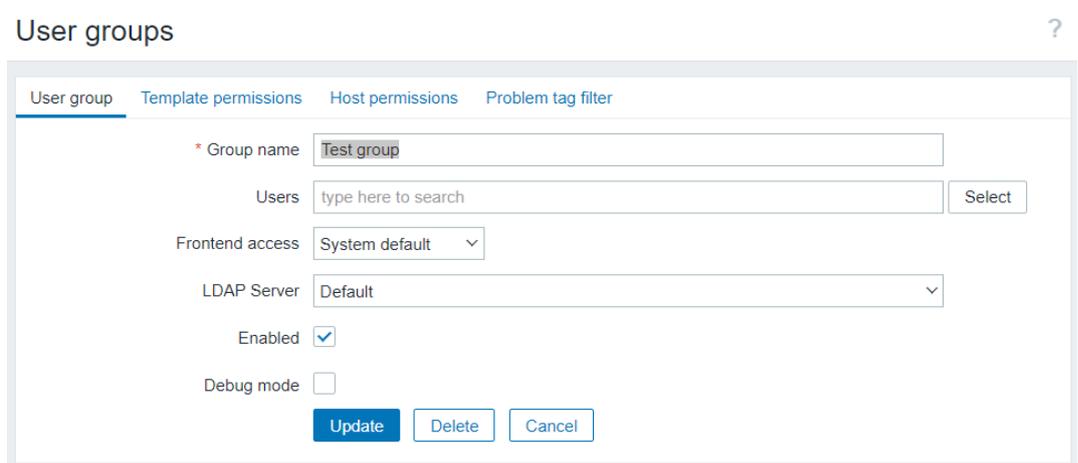
5. Click **Update** to complete changes.

Note The following steps are optional, they have to be done to add a user to a user group to send email to all users of this group.

- From the **Users** menu, click the **User groups** tab. The **User groups** page opens.



- Select the user group required. A new page opens.



- In the **Users** section, click Select. The **Users** pop-up windows opens.



9. Select the user to be added in the list.

<input type="checkbox"/>	Username	Name	Last name
<input type="checkbox"/>	Admin	Zabbix	Administrator
<input type="checkbox"/>	guest		
<input checked="" type="checkbox"/>	Test		

10. Click **Select**.

The user is displayed in the **Users** field.

User group Template permissions Host permissions Problem tag filter

* Group name

Users
type here to search

Frontend access

LDAP Server

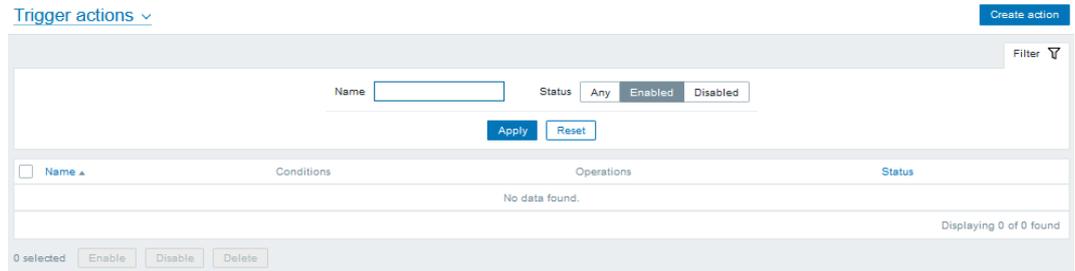
Enabled

Debug mode

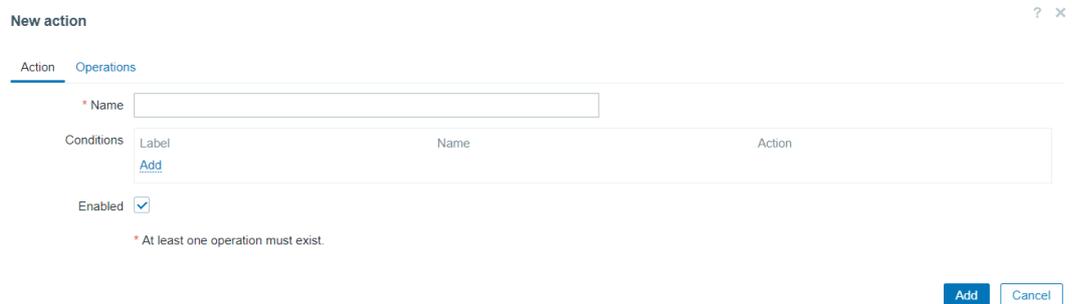
11. Click **Update**

7.3. Creating a trigger action

1. From the **Alert** menu, click **Actions > Trigger actions**. The **Trigger actions** page opens.



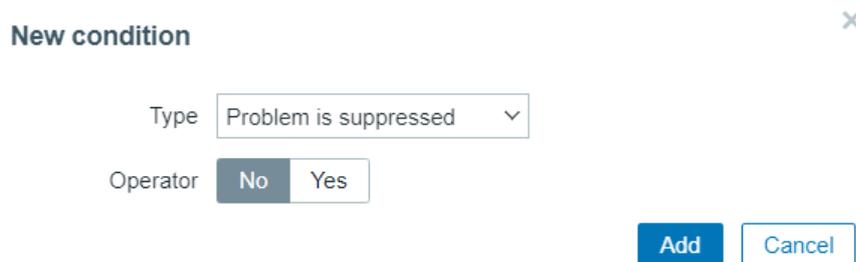
2. Click **Create action**. A **New action** pop-window opens.



3. Complete the **Name** field.

To set conditions for sending the mail, perform the following steps, otherwise go directly to step 7.

4. In the **Conditions** section, click **Add**. A **New condition** pop-up windows opens.



5. Choose **Type** in the drop-down list and complete condition value.

Example

New condition ✕

Type ▼

Operator

Severity

6. Click **Add**. The condition is displayed in the **Conditions** section.

New action ? ✕

Action Operations

* Name

Conditions

Label	Name	Action
A	Trigger severity is greater than or equals <i>Warning</i>	Remove

[Add](#)

Enabled

* At least one operation must exist.

7. Click the **Operations** tab.

New action ? ✕

Action Operations

* Default operation step duration

Operations

Steps	Details	Start in	Duration	Action
Add				

Recovery operations

Details	Action
Add	

Update operations

Details	Action
Add	

Pause operations for symptom problems

Pause operations for suppressed problems

Notify about canceled escalations

* At least one operation must exist.

8. In the **Operations** section, click **Add**. The **Operation details** pop-up window opens.

Operation details ✕

Operation

* At least one user or user group must be selected.

Send to user groups

Send to users

Send only to

Custom message

9. In the **Operation details** window, perform the following actions:
- a. Add the message recipient.
If the recipient is a user group:
 - i. In the **Send to User groups** section, click **Select**. The **User groups** pop-up window opens.
 - ii. Select the user groups required.If the recipient is a user:
 - i. In the **Send to Users** section, click **Select**. The **Users** pop-up window opens.
 - ii. Select the users required.

- b. From the **Send only to** drop-down list, select the media type previously created.

Operation details ✕

Operation Send message

Steps - (0 - infinitely)

Step duration  (0 - use action default)

* At least one user or user group must be selected.

Send to user groups

Send to users

Send only to

Custom message

Label	Name	Action
Add		

- c. Custom the message if needed.

Operation details ✕

Operation Send message

Steps - (0 - infinitely)

Step duration  (0 - use action default)

* At least one user or user group must be selected.

Send to user groups

Send to users

Send only to

Custom message

Subject

Message

Label	Name	Action
Add		

d. Click **Add**.

Example

Actions

Action Operations 1

* Default operation step duration 1h

Operations

Steps	Details	Start in	Duration	Action
1	Send message to users: Admin (Zabbix Administrator) via Email example	Immediately	Default	Edit Remove

Recovery operations

Details	Action

Update operations

Details	Action

Pause operations for suppressed problems

Notify about canceled escalations

* At least one operation must exist.

Add Cancel

10. Click **Add** to complete changes.

The action is created.

Example

Trigger actions Create action

✓ Action added

Name Status Any Enabled Disabled Filter

Apply Reset

Name	Conditions	Operations	Status
Action trigger example		Send message to users: Admin (Zabbix Administrator) via Email example	Enabled

0 selected Enable Disable Delete

An email will be sent for each problem having the minimum severity level.

Time	Severity	Recovery time	Status	Info	Host	Problem
14:55:22	Warning	15:04:45	RESOLVED		MESCA5_12	CPU0_Inlet_Temp lower non critical threshold

Problem CPU0_Inlet_Temp lower critical threshold

Problem started at 14:55:22 on 2023.02.10 Problem name: CPU0_Inlet_Temp lower critical threshold

Host: MESCA5_12

Severity: High

Original problem ID: 339198

