

# Management Console 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 2020

Printed in France

## **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**

**July 2020**

**Bull Cedoc  
357 avenue Patton  
BP 20845  
49008 Angers Cedex 01  
FRANCE**

*The information in this document is subject to change without notice. Bull 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

<b>Preface</b> .....	<b>p-1</b>
Intended Readers .....	p-1
<b>Chapter 1. Installing the MISM console</b> .....	<b>1-1</b>
1.1. Introduction .....	1-1
1.2. Installing / Updating the MISM console .....	1-2
1.3. Controlling the MISM console .....	1-4
1.4. Changing the connection certificate .....	1-5
1.5. Configuring a proxy server .....	1-6
<b>Chapter 2. Controlling resources</b> .....	<b>2-1</b>
2.1. Logging in .....	2-2
2.2. Console description .....	2-3
2.2.1. Console overview .....	2-3
2.2.2. Delivery content .....	2-4
2.3. Adding resources .....	2-5
2.3.1. Creating an inventory .....	2-5
2.3.2. Adding a host to an inventory .....	2-7
2.3.3. Creating a group of hosts in an inventory .....	2-8
2.4. Controlling resources .....	2-10
2.4.1. Available job templates .....	2-10
2.4.2. Launching a job .....	2-13
2.4.3. Scheduling a job .....	2-16
2.5. Adding security .....	2-19
2.5.1. Creating a password for the BullSequana Edge Vault .....	2-19
2.5.2. Creating an encrypted password for a host .....	2-20
2.5.3. Deleting an encrypted password .....	2-21
2.6. Setting up email alerts .....	2-22
2.6.1. Creating an email notification template .....	2-22
2.6.2. Assigning a notification to a job template .....	2-24
2.7. Performing basic operations .....	2-25
2.7.1. Performing power operations .....	2-25
2.7.2. Updating firmware .....	2-26
2.7.3. Enabling syslog forwarding .....	2-28
<b>Chapter 3. Monitoring resources</b> .....	<b>3-1</b>
3.1. Logging in .....	3-2
3.2. Console description .....	3-3
3.2.1. Console overview .....	3-3
3.2.2. Delivery content .....	3-5
3.3. Preliminary configuration .....	3-5
3.3.1. Enabling automatic inventory .....	3-5
3.3.2. Renaming the Zabbix server host .....	3-5

3.4.	Managing Atos LLD template .....	3-7
3.4.1.	Template description .....	3-7
3.4.2.	Importing the Atos LLD template .....	3-7
3.5.	Adding resources .....	3-9
3.5.1.	Adding hosts with the zabbix discovery service .....	3-9
3.5.2.	Adding a host manually .....	3-14
3.5.3.	Linking a host to the Atos LLD template .....	3-15
3.5.4.	Filling Atos template macros .....	3-16
3.6.	Adding security .....	3-18
3.6.1.	Activating PSK security .....	3-18
3.6.2.	Enabling PSK security for a host .....	3-18
3.6.3.	Creating an encrypted password for a host .....	3-19
3.7.	Enabling syslog forwarding .....	3-21
3.7.1.	Importing the Atos Rsyslog template .....	3-21
3.7.2.	Linking the Zabbix server host to the Atos Rsyslog template ....	3-22
3.7.3.	Displaying the logs .....	3-23
3.8.	Configuring nmap .....	3-24
3.8.1.	Creating a nmap discovery rule .....	3-24
3.8.2.	Creating a nmap action .....	3-25
3.9.	Setting up email alerts .....	3-29
3.9.1.	Configuring an mail server .....	3-29
3.9.2.	Creating an action .....	3-31
3.9.3.	Configuring the user .....	3-34
3.10.	Setting up SMS alerts .....	3-36
3.10.1.	Configuring the SMS .....	3-36
3.10.2.	Creating an action .....	3-39
3.10.3.	Configuring the user .....	3-42
3.11.	Monitoring resources .....	3-45
3.11.1.	Dashboard .....	3-45
3.11.2.	Problems .....	3-45
3.11.3.	Overview .....	3-45
3.11.4.	Web .....	3-45
3.11.5.	Latest data .....	3-46
3.11.6.	Graphs .....	3-46
3.11.7.	Screens .....	3-46
3.11.8.	Maps .....	3-46
3.11.9.	Discovery .....	3-46
3.11.10.	Services .....	3-46

---

## Preface

This guide explains how to use the Machine Intelligence System Management (MISM) console to manage BullSequana Edge servers.

---

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

---

---

## Intended Readers

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



---

## Chapter 1. Installing the MISM console

### 1.1. Introduction

The Machine Intelligence System Management (MISM) console allows the user to manage BullSequana Edge servers.

MISM is delivered as docker containers and is based on two open-source software:

- Ansible Tower to control servers through a graphical user interface
- Zabbix to monitor servers through a graphical user interface

## 1.2. Installing / Updating the MISM console

This section explains how to install the Machine Intelligence System Management (MISM) console on the system selected to host it.

---

**Important** On an existing installation, tower-cli should be installed to run add\_awx\_playbooks.sh.

---

### Prerequisites

Docker CE version 17.12.0 or higher is installed and running

<https://docs.docker.com/install/>

Docker Compose version 1.24.0 or higher is installed

<https://docs.docker.com/compose/install/>

The mism\_<version>.gz package is available

### Estimated operation time

15 minutes

### Procedure

For a first installation or to update an existing installation, perform the following operations:

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

```
$ tar xvf mism_<version>.gz
```

4. Run the following command.

```
$ ./install.sh
```

---

**Notes**

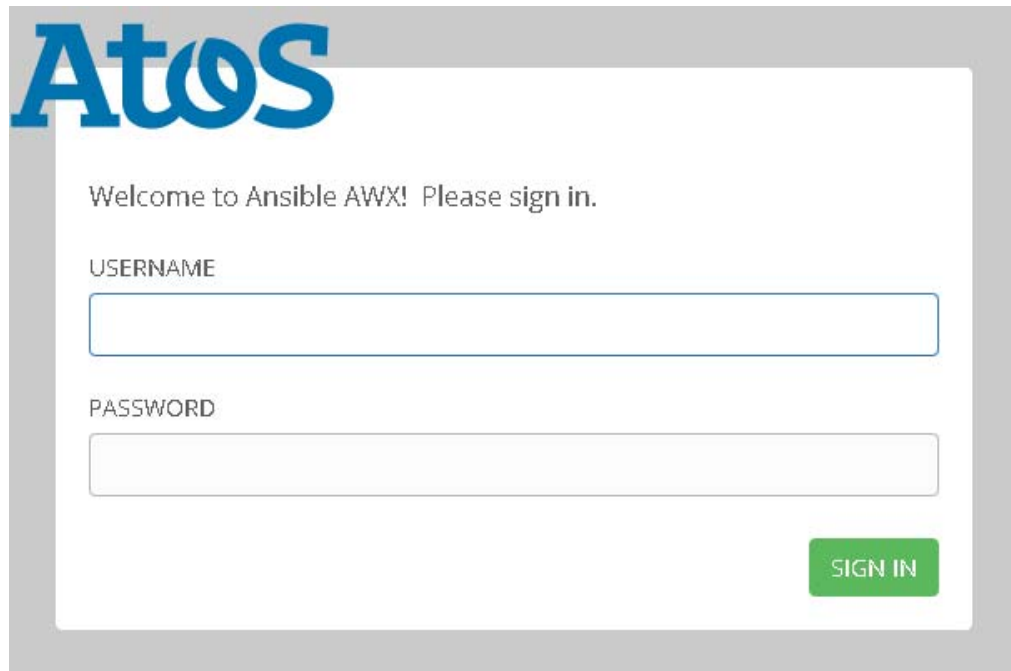
- Performed on an existing installation, this operation preserves user data such as inventories and user accounts
- Ansible installation is optional

---

5. When the request to confirm the installation of Ansible appears, answer Yes or No as required.
6. Open a web browser.
7. Connect to the MISM console by entering the name or IP address of the MISM console in the address bar, using the https protocol.



8. Wait until the update is complete and the authentication page opens.

The screenshot shows the Atos logo in blue at the top left. Below it, the text "Welcome to Ansible AWX! Please sign in." is displayed. There are two input fields: "USERNAME" and "PASSWORD". The "PASSWORD" field is masked with dots. A green "SIGN IN" button is located at the bottom right of the form area.

9. Run the following command.

```
$ ./add_awx_playbooks.sh
```

**Note** Performed on an existing installation, this operation preserves any playbook created by the user. However, any playbook from the BullSequana Edge Playbooks project that has been modified by the user is restored to its original state.

## 1.3. Controlling the MISM console

---

**Note** The commands are located in the MISM installation directory.

---

- To get the version of the installed MISM console, run the following command:

```
$ ./get_mism_version.sh
```

- To uninstall the MISM console, run the following command:

```
$ ./uninstall.sh
```

- To start the MISM console, run the following command:

```
$ ./start.sh
```

- To stop the MISM console, run the following command:

```
$ ./stop.sh
```

## 1.4. Changing the connection certificate

1. Stop the MISM console.
  - a. Go to the MISM installation directory.
  - b. Run the following command.

```
$ ./stop.sh
```

2. Go to the SSL directory.

```
$ cd ansible/awx_ssl
```

3. Generate 2048 private key.

- Without a passphrase:

```
$ openssl genrsa -out nginx.key 2048
```

- With a passphrase:

```
$ openssl genrsa -out nginx.key -passout stdin 2048
```

The nginx.key file is generated.

4. Generate a request for a csr certificate.

```
$ openssl req -sha256 -new -key nginx.key -out nginx.csr -subj '/CN=awx.local'
```

The nginx.csr file is generated.

5. Generate a crt certificate.

```
$ openssl x509 -req -sha256 -days 365 -in nginx.csr -signkey nginx.key -out nginx.crt
```

The nginx.crt file is generated.

6. Start the MISM console.
  - a. Go to the MISM installation directory.
  - b. Run the following command.

```
$ ./start.sh
```

## 1.5. Configuring a proxy server

There is no proxy server delivered with the MISM console.

To configure a proxy server for the MISM console, perform the following operations:

1. Stop the MISM console.
  - a. Go to the MISM installation directory.
  - b. Run the following command.

```
$ ./stop.sh
```

2. Open the `docker-compose-mism.yml` file with a text editor.
3. In the `environment` sub-section of the `awx_web` section, add the following lines:

```
-----  
http_proxy: http://<proxy>:<port number>  
https_proxy: https://<proxy>:<port number>  
no_proxy: 127.0.0.1,localhost,zabbix-web,zabbix-server,zabbix-agent,awx_web,  
awx_task,rabbitmq,postgres,memcached, <IP address>  
-----
```

4. In the `environment` sub-section of the `awx_task` section, add the following lines:

```
-----  
http_proxy: http://<proxy>:<port number>  
https_proxy: https://<proxy>:<port number>  
no_proxy: 127.0.0.1,localhost,zabbix-web,zabbix-server,zabbix-agent,awx_web,  
awx_task,rabbitmq,postgres,memcached, <IP address>  
-----
```

5. Save and close the `docker-compose-mism.yml` file.
6. Start the MISM console.

```
$ ./start.sh
```

---

## Chapter 2. Controlling resources

To control systems, the Machine Intelligence System Management (MISM) console uses the Ansible Tower framework. Ansible Tower is a graphically-enabled framework accessible via a web interface and a REST API endpoint for Ansible, the open source IT orchestration engine.

---

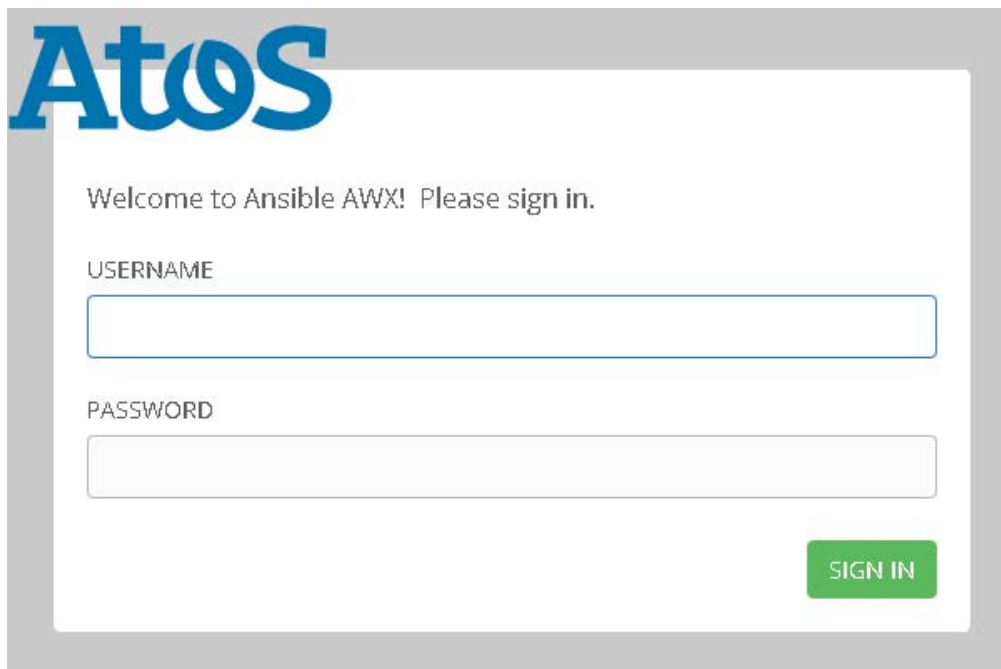
**Important** Consult the full Ansible Tower documentation before using the MISM console:  
<https://docs.ansible.com/ansible-tower/>

---

## 2.1. Logging in

### Procedure

1. Launch the web browser and enter the name or IP address of the MISM console using the https protocol. The authentication page opens.



Controlling console	
Username	Default name: mism
Password	Default password: mismpass

2. Complete the **Username** and **Password** fields and click **Sign in**. The **Dashboard** page opens.

### What to do if an incident occurs?

If the connection to the MISM 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)

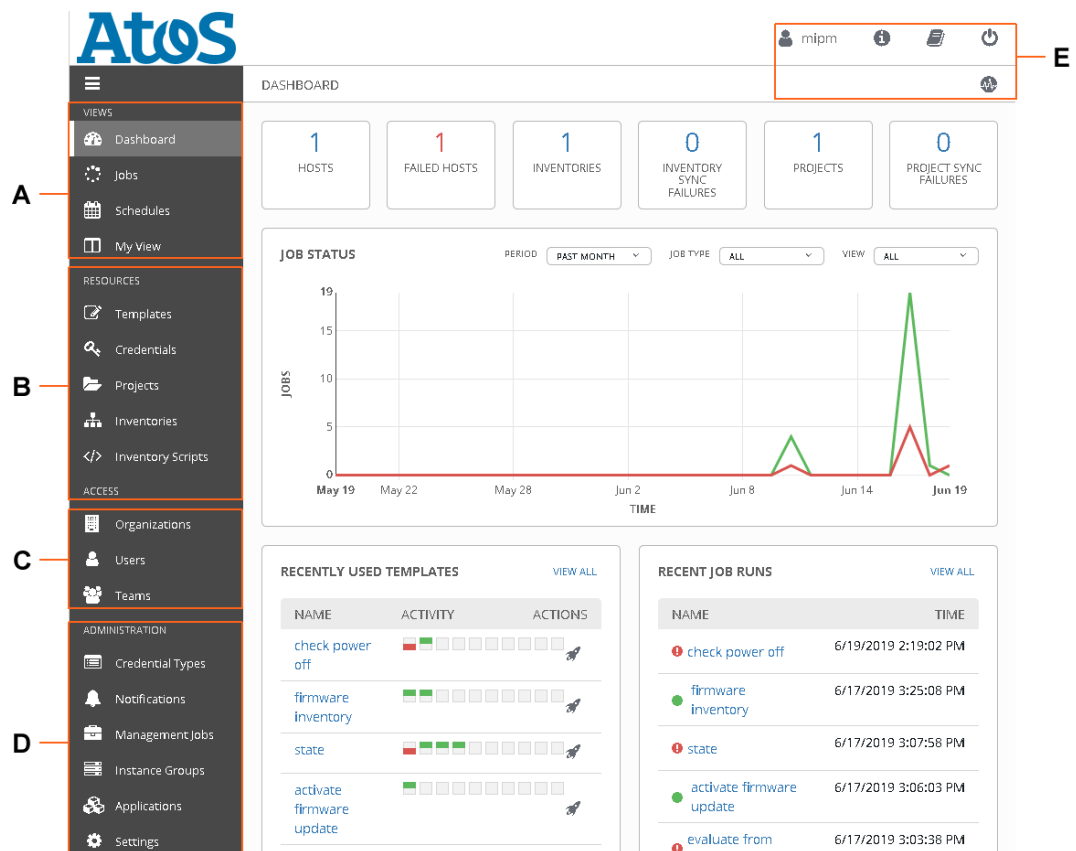
---

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

---

## 2.2. Console description

### 2.2.1. Console overview



Mark	Description
A	Views
B	Resources
C	Access
D	Administration
E	Quick access

## Features

Area	Description	Features
Quick access	Provides rapid access to frequently used features	User Account
		About
		Ansible Tower Documentation
		Log Out
		Activity Stream
Views	Provides access to resource monitoring features	Dashboard
		Jobs
		Schedules
		My View
Resources	Provides access to resource management and configuration features	Templates
		Credentials
		Projects
		Inventories
		Inventory Scripts
Access	Provides access to user management and permission setting features	Organizations
		Users
		Teams
Administration	Provides access to various administrative options	Credential Types
		Notifications
		Management Jobs
		Instance Groups
		Applications
		Settings

### 2.2.2. Delivery content

On delivery, the monitoring console contains the following elements:

- The BullSequana Edge Playbooks project, which contains the delivered playbooks
- A collection of job templates, which are based on the provided playbooks
- The BullSequana Edge inventory, given as an example
- The Bull organization
- The BullSequana Edge group
- The BullSequana Edge Vault credential

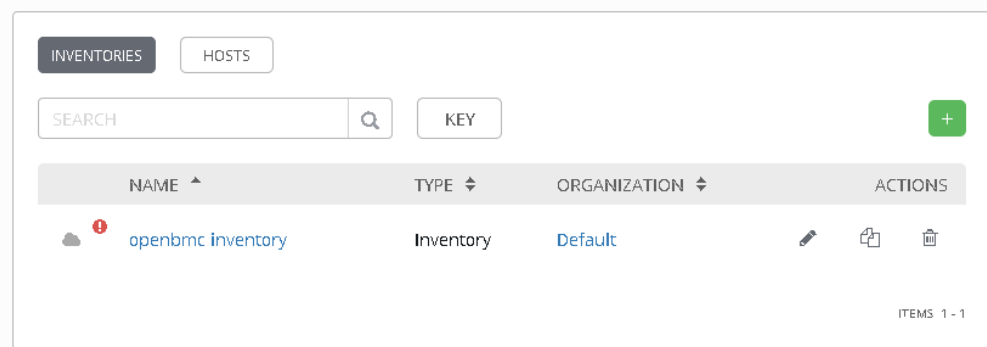


## 2.3. Adding resources

### 2.3.1. Creating an inventory

**Note** The Openbmc inventory is delivered as an example of how to set up an inventory.

1. From the left navigation bar, click **Inventories**. The **Inventories** page opens.



2. Click the green + and select **Inventory**. The **New Inventory** page opens.

The screenshot shows the 'NEW INVENTORY' form. It has tabs for DETAILS, PERMISSIONS, GROUPS, HOSTS, SOURCES, and COMPLETED JOBS. The DETAILS tab is active. Fields include: NAME (required), DESCRIPTION, ORGANIZATION (required, with a dropdown showing 'Default'), INSIGHTS CREDENTIAL, and INSTANCE GROUPS. There is a VARIABLES section with a toggle for YAML/JSON and an EXPAND button. At the bottom are CANCEL and SAVE buttons.

3. Complete the **Name** and **Organization** fields.

4. Complete the **Variables** field.

Variable	Description	BullSequana Edge inventory value
forceoff	Indicates if powering the server off is necessary during a job. Possible values: <ul style="list-style-type: none"> <li>• True: the host is automatically powered off.</li> <li>• False: the host is not automatically powered off and the BIOS or CPLD update is effective only after the next power cycle.</li> </ul>	True
power_cap	Provides the maximum value allowed for power consumption	Not defined
poweroff_countdown	Indicates the delay before checking that the host is successfully powered off (in seconds).	15
poweron_countdown	Indicates the delay before checking that the host is successfully powered on (in seconds).	15
reboot	Indicates if rebooting the BMC is necessary during a job. Possible values: <ul style="list-style-type: none"> <li>• True: the BMC reboots automatically.</li> <li>• False: the BMC does not automatically reboot and the BMC update is effective only after the next reboot.</li> </ul>	True
reboot_countdown	Indicates the delay before checking that the BMC rebooted successfully (in minutes).	3
rsyslog_server_ip	Provide the network parameters necessary for rsyslog	0.0.0.0
rsyslog_server_port		514
technical_state_path	Provides the path to the Technical State file when updating firmware	/host/mnt

**Note** If these variables are not defined in the inventory, they must be defined as extra variables when launching a job.

5. Complete the other fields as needed.

6. Click **Save**.

### 2.3.2. Adding a host to an inventory

1. From the **Inventories** page, click the newly created inventory. The inventory page opens.

My first inventory

DETAILS PERMISSIONS GROUPS HOSTS SOURCES COMPLETED JOBS

\* NAME My first inventory DESCRIPTION \* ORGANIZATION Default

INSIGHTS CREDENTIAL INSTANCE GROUPS

VARIABLES ? YAML JSON EXPAND

```
1 forceoff: True
2 reboot: True
3
4 # Set a path to a Bull Technical State file
5 technical_state_path: /mnt
6
```

CANCEL SAVE

2. Click **Hosts**.
3. Click the green + button. The **Create Host** page opens.

CREATE HOST ON

DETAILS FACTS GROUPS COMPLETED JOBS

\* HOST NAME ? DESCRIPTION

VARIABLES ? YAML JSON EXPAND

```
1 ---
```

CANCEL SAVE

4. Complete the **Host Name** field with the IP address of the server to be added.

- Complete the **Variables** field with the mandatory variables.

VARIABLES YAML JSON EXPAND

```

1 ---
2 baseuri: "{{ inventory_hostname }}"
3 username: <username>
4 password: <pwd>

```

Mandatory host variables	
baseuri	Write "{{inventory_hostname}}"
username	Write the host BMC username
password	Write the host BMC password

**Note** If the host BMC password is not indicated here, set up the job templates to prompt for it as an extra variable at launch.

**See** 2.5. Adding security if a encrypted password is necessary.

- Click **Save**.

### 2.3.3. Creating a group of hosts in an inventory

- From the **Inventories** page, click the inventory to be edited. The inventory page opens.

My first inventory ✕

DETAILS PERMISSIONS GROUPS HOSTS SOURCES COMPLETED JOBS

\* NAME My first inventory DESCRIPTION ORGANIZATION Q Default

INSIGHTS CREDENTIAL INSTANCE GROUPS ? Q

VARIABLES YAML JSON EXPAND

```

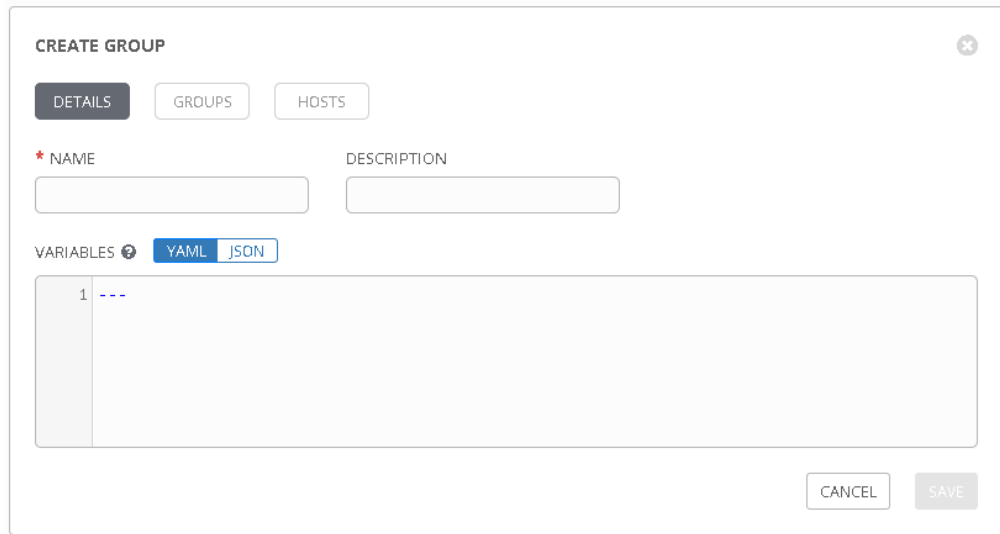
1 forceoff: True
2 reboot: True
3
4 # Set a path to a Bull Technical State file
5 technical_state_path: /mnt
6

```

CANCEL SAVE

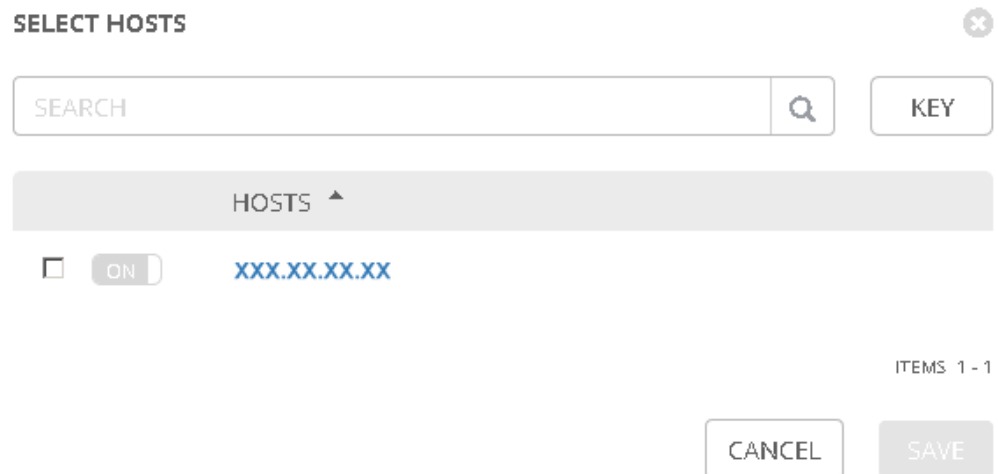
- Click **Groups**.

- Click the green + button. The **Create Group** page opens.



The screenshot shows a 'CREATE GROUP' form with a close button in the top right. It has three tabs: 'DETAILS' (selected), 'GROUPS', and 'HOSTS'. Under 'DETAILS', there are two input fields: 'NAME' (required, marked with a red asterisk) and 'DESCRIPTION'. Below these is a 'VARIABLES' section with a help icon and two tabs: 'YAML' (selected) and 'JSON'. A text area for variables is shown with a line number '1' and a dashed line. At the bottom right are 'CANCEL' and 'SAVE' buttons.

- Complete the required fields and click **Save**.
- Click **Hosts**.
- Click the green + button and select **Existing Host**. The **Select Hosts** window opens.



The screenshot shows a 'SELECT HOSTS' window with a close button in the top right. It features a search bar with a 'SEARCH' placeholder and a magnifying glass icon, and a 'KEY' button. Below is a list of hosts, with the first one expanded to show a checkbox, an 'ON' toggle, and the IP address 'xxx.xx.xx.xx'. At the bottom right, it says 'ITEMS 1 - 1' and has 'CANCEL' and 'SAVE' buttons.

- Select the hosts to be added to the group and click **Save**.

## 2.4. Controlling resources

BullSequana Edge servers are controlled by launching jobs from different job templates.

### 2.4.1. Available job templates

The MISM console is delivered with a collection of job templates.

Name	Description	Necessary variables
Activate firmware updates	Activates newly uploaded firmware	<ul style="list-style-type: none"><li>reboot</li><li>forceoff</li></ul>
BIOS Boot Mode	Retrieve BIOS boot information	None
BIOS Boot Source		
Check BMC alive	Checks that the BMC is running	
Check critical high and low alarms	Checks for high and low critical alarms in the system	
Check Power Off	Check the system power state	
Check Power On		
Check Rsyslog Server IP and Port	Checks that the syslog server IP address and port are identical to the ones defined in the inventory variables.	<ul style="list-style-type: none"><li>rsyslog_server_ip</li><li>rsyslog_server_port</li></ul>
Check warning high and low alarms	Checks for high and low warning alarms in the system	None
Delete firmware image	Deletes a firmware image uploaded on the BMC	image
Evaluate firmware update from Technical State	Details what will be updated by the Technical State	technical_state_path
Firmware inventory - Active	Lists the firmware that has been uploaded and activated	None
Firmware inventory - Ready	Lists the firmware that has been uploaded but not activated	
FRU	Returns FRU information	
Get Rsyslog Server IP and Port	Retrieves syslog server information	
Immediate Shutdown	Powers off the system without waiting for software to stop	
LED	Returns the state of the module identification LED	
Logs	Retrieves the system logs	
Network	Lists the network interfaces	

Name	Description	Necessary variables
Orderly Shutdown	Stops all software on the system before removing power	
Power Cap	Returns the maximum value allowed for power consumption	None
Power On	Powers on the system	
Reboot BMC	Stops and starts the BMC again	
Rsyslog Server IP and Port	Retrieves syslog server information	
Sensors	Retrieves the sensor information	
Set BIOS Boot Mode to Regular	Select the BIOS boot mode	
Set BIOS Boot Mode to Safe		
Set BIOS Boot Mode to Setup		
Set BIOS Boot Source to Default	Select the BIOS boot source	
Set BIOS Boot Source to Disk		
Set BIOS Boot Source to External Media		
Set BIOS Boot Source to Network		
Set LED off	Turns the module identification LED off	
Set LED on	Turns the module identification LED on	
Set Power Cap off	Removes the possibility of setting a maximum value for power consumption	
Set Power Cap on	Sets a maximum value for power consumption	power_cap
Set Rsyslog Server IP	Set up the syslog server	rsyslog_server_ip
Set Rsyslog Server Port		rsyslog_server_port
State BMC	Check the state of the system components	None
State Chassis		
State Host		
System	Returns system information.	
Update firmware from file	Updates firmware from a file.	<ul style="list-style-type: none"><li>file_to_update</li><li>reboot</li><li>forceoff</li></ul>

Name	Description	Necessary variables
Update firmware from Technical State	Updates all the system firmware from the Technical State.	<ul style="list-style-type: none"> <li>• technical_state_path</li> <li>• reboot</li> <li>• forceoff</li> </ul>
Upload firmware images from Technical State	Uploads all the system firmware from the Technical State	technical_state_path



## 2.4.2. Launching a job

This section explains how to launch a job manually. Jobs can also be scheduled to launch automatically.

**See** The Ansible Tower documentation for more information:  
<https://docs.ansible.com/ansible-tower/>

1. Navigate to the **My View** or **Templates** page to display the job template list.

TEMPLATES		15
SEARCH	Q	KEY
		Compact Expanded
activate firmware update	Job Template	
check critical alarms	Job Template	
check power off	Job Template	
check power on	Job Template	
evaluate from technical state	Job Template	
firmware inventory	Job Template	
FRU	Job Template	
get logs	Job Template	
power off	Job Template	

- Click the required job template. The job template page opens.

**firmware inventory** ✕

DETAILS PERMISSIONS NOTIFICATIONS COMPLETED JOBS SCHEDULES **ADD SURVEY**

* NAME <input type="text" value="firmware inventory"/>	DESCRIPTION <input type="text"/>	* JOB TYPE <span>?</span> <input type="checkbox"/> PROMPT ON LAUNCH <input type="text" value="Run"/>
* INVENTORY <span>?</span> <input type="checkbox"/> PROMPT ON LAUNCH <input type="text" value="openbmc inventory"/>	* PROJECT <span>?</span> <input type="text" value="openbmc project"/>	* PLAYBOOK <span>?</span> <input type="text" value="firmware/get_firmware_invent..."/>
CREDENTIAL <span>?</span> <input type="checkbox"/> PROMPT ON LAUNCH <input type="text"/>	FORKS <span>?</span> <input type="text" value="0"/>	LIMIT <span>?</span> <input type="checkbox"/> PROMPT ON LAUNCH <input type="text"/>
* VERBOSITY <span>?</span> <input type="checkbox"/> PROMPT ON LAUNCH <input type="text" value="2 (More Verbose)"/>	JOB TAGS <span>?</span> <input type="checkbox"/> PROMPT ON LAUNCH <input type="text"/>	SKIP TAGS <span>?</span> <input type="checkbox"/> PROMPT ON LAUNCH <input type="text"/>
LABELS <span>?</span> <input type="text"/>	INSTANCE GROUPS <span>?</span> <input type="text"/>	JOB SLICING <span>?</span> <input type="text" value="1"/>
TIMEOUT <span>?</span> <input type="text" value="0"/>	SHOW CHANGES <span>?</span> <input type="checkbox"/> PROMPT ON LAUNCH <input type="text" value="OFF"/>	OPTIONS <input type="checkbox"/> ENABLE PRIVILEGE ESCALATION <span>?</span> <input type="checkbox"/> ALLOW PROVISIONING CALLBACKS <span>?</span> <input type="checkbox"/> ENABLE CONCURRENT JOBS <span>?</span> <input type="checkbox"/> USE FACT CACHE <span>?</span>

EXTRA VARIABLES ?   ☐ PROMPT ON LAUNCH

1 ---

CANCEL SAVE LAUNCH

- Complete the **Inventory** field with the inventory containing the hosts to be manipulated by the job.
- If needed, complete the **Limit** field with a group in the selected inventory to further constrain the lists of hosts to be manipulated by the job.
- Complete the **Extra variables** field.

---

**See** 2.4.1. Available job templates to review the variables needed for each job.

---

- If the host password has not been provided as a host variable, select **Prompt at launch** next to the **Extra variables** field. The user will be asked to give the password as a variable when the job launches.
- Click **Save**.

8. Click **Launch**. The **Jobs** page opens.

The screenshot displays the Ansible Tower interface. On the left, the 'DETAILS' panel for a job named 'firmware inventory' shows a 'Successful' status. Key details include: Started at 6/21/2019 6:01:36 PM, Finished at 6/21/2019 6:01:58 PM, Job Template 'firmware inventory', Job Type 'Run', Launched by 'mipm', Inventory 'openbmc inventory', Project 'openbmc project', Playbook 'firmware/get\_firmware\_inventory.yml', Verbosity '2 (More Verbose)', Environment '/var/lib/awx/venv/ansible', Execution Node 'awx', and Instance Group 'tower'. The 'EXTRA VARIABLES' section is currently empty.

The main panel shows the job's output in a text window. The output includes the Ansible version (2.9.0.dev0), configuration file path (/etc/ansible/ansible.cfg), module search paths, and the execution of the 'firmware inventory' playbook. The output is structured as follows:

```
1 ansible-playbook 2.9.0.dev0
2   config file = /etc/ansible/ansible.cfg
3   configured module search path = [u'/var/lib/awx/.ansible/plugins/modules', u'/usr/share/ansible/plugins/modules']
4   ansible python module location = /usr/lib/python2.7/site-packages/ansible
5   executable location = /usr/bin/ansible-playbook
6   python version = 2.7.5 (default, Oct 30 2018, 23:45:53) [GCC 4.8.5 20150623 (Red Hat 4.8.5-36)]
7   Using /etc/ansible/ansible.cfg as config file
8
9 PLAYBOOK: get_firmware_inventory.yml
10 *****
11 1 plays in firmware/get_firmware_inventory.yml
12
13 PLAY [Firmware Update] 18:01:48
14 *****
15 META: ran handlers
16
17 TASK [Create Auth token] 18:01:48
18 *****
19 task path: /var/lib/awx/projects/openbmc/firmware/get_firmware_inventory.yml:8
```

9. Consult the process and output of the job in the text window.

10. Click ... to display hidden lines.

### 2.4.3. Scheduling a job

This section explains how to schedule a job so that it is launched automatically.

---

**Note** Job schedules are created from template, project or inventory resources.

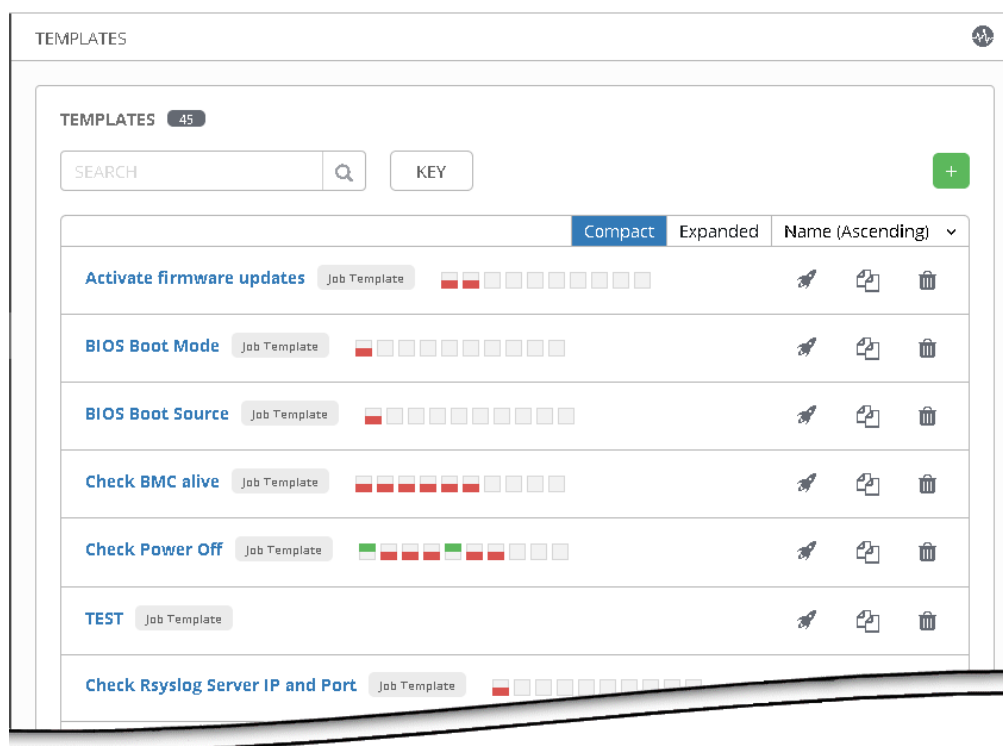
---

**See** The Ansible Tower documentation for more information:  
<https://docs.ansible.com/ansible-tower/>

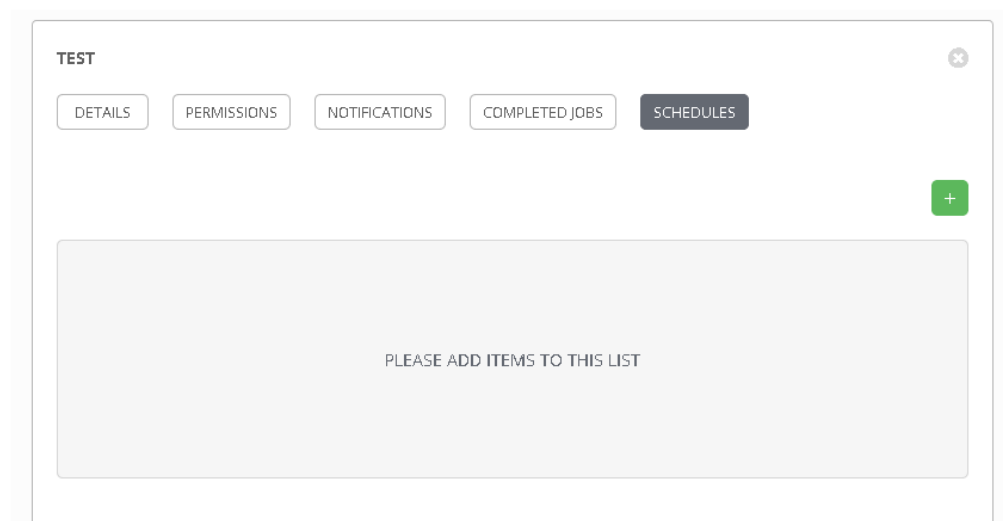
---

1. From the left navigation bar, click a resource (Templates, Projects or Inventories). A new page opens.

#### Templates example



2. Click a resource.



- Click the **Schedules** tab.
- Complete the fields as required.

### Example

MySchedule

\* NAME

MySchedule

\* START DATE

07/3/2020

\* START TIME (HH24:MM:SS)

0

:

0

:

0

\* LOCAL TIME ZONE

Europe/Paris

\* REPEAT FREQUENCY

Month

FREQUENCY DETAILS

\* EVERY

1

MONTH

S

\* ON DAY

1

\* ON THE

first

Sunday

\* END

After

\* OCCURRENCES

3

SCHEDULE DESCRIPTION

every month on the 1st for 3 times

OCCURRENCES (Limited to first 10)

DATE FORMAT

☒ LOCAL TIME ZONE
 ☐ UTC

04-01-2020 00:00:00

05-01-2020 00:00:00

06-01-2020 00:00:00

CANCEL

SAVE

**Important** The schedules must be set in UTC time.

- Click **Save** to complete changes.

The schedule is created for the resource.

TEST

DETAILS

PERMISSIONS

NOTIFICATIONS

COMPLETED JOBS

SCHEDULES

SEARCH

Q

KEY

+

NAME	FIRST RUN	NEXT RUN	FINAL RUN	ACTIONS
<input checked="" type="checkbox"/> MySchedule	1/4/2020 00:00:00	1/4/2020 00:00:00	1/6/2020 00:00:00	<div>✎</div> <div>🗑</div>

ITEMS 1 - 1

- Use the toggle button to enable or disable the schedule.

Chapter 2. Controlling resources 2-17

- From the left navigation bar, click **Schedules** to manage the scheduled jobs.

SCHEDULED JOBS 5

SEARCH

KEY

NAME	TYPE	NEXT RUN	ACTIONS
<input checked="" type="checkbox"/> MySchedule	Playbook Run	1/4/2020 00:00:00	
<input checked="" type="checkbox"/> Cleanup Expired Sessions	Management Job		
<input checked="" type="checkbox"/> Cleanup Expired OAuth 2 Tokens	Management Job		
<input checked="" type="checkbox"/> Cleanup Job Schedule	Management Job	8/3/2020 09:37:41	
<input checked="" type="checkbox"/> Cleanup Activity Schedule	Management Job	10/3/2020 09:37:41	

ITEMS 1 - 5

## 2.5. Adding security

The BullSequana Edge Vault can be used to store encrypted passwords. On delivery, it is already associated with all the delivered job templates as a credential.

The screenshot shows the configuration page for a job template named "BIOS Boot Mode". The page has tabs for DETAILS, PERMISSIONS, NOTIFICATIONS, COMPLETED JOBS, SCHEDULES, and ADD SURVEY. The configuration is organized into several sections:

- NAME:** BIOS Boot Mode
- DESCRIPTION:** BIOS Boot Mode
- JOB TYPE:** Run
- INVENTORY:** BullSequana Edge Inventory
- PROJECT:** BullSequana Edge Playbooks
- PLAYBOOK:** firmware/get\_bios\_boot\_mode.yml
- CREDENTIAL:** BullSequana Edge Vault | bullsequana\_edge\_password
- FORKS:** 0
- LIMIT:** 0
- VERBOSITY:** 0 (Normal)
- JOB TAGS:**
- SKIP TAGS:**
- LABELS:**
- INSTANCE GROUPS:**
- JOB SLICING:** 1
- TIMEOUT:** 0
- SHOW CHANGES:** (toggle switch)
- OPTIONS:**
  - ENABLE PRIVILEGE ESCALATION
  - ALLOW PROVISIONING CALLBACKS
  - ENABLE CONCURRENT JOBS
  - USE FACT CACHE

### 2.5.1. Creating a password for the BullSequana Edge Vault

The BullSequana Edge Vault initially has no defined password. To create one, perform the following actions:

1. From the left navigation bar, click **Credentials**. The **Credentials** page opens.

The screenshot shows the CREDENTIALS page with a search bar and a table of credentials. The table has columns for NAME, KIND, OWNERS, and ACTIONS.

NAME	KIND	OWNERS	ACTIONS
Demo Credential	Machine	mism	[edit] [copy] [delete]
BullSequana Edge Vault	Vault	Bull	[edit] [copy] [delete]

ITEMS 1 - 2

2. Click **BullSequana Edge Vault**. The **BullSequana Edge Vault** page opens.

The screenshot shows the configuration page for the BullSequana Edge Vault. It has tabs for DETAILS and PERMISSIONS. The configuration includes:

- NAME:** BullSequana Edge Vault
- DESCRIPTION:** BullSequana Edge Vault associated to
- ORGANIZATION:** Bull
- CREDENTIAL TYPE:** Vault
- TYPE DETAILS:**
  - VAULT PASSWORD:** (input field with a toggle for "Prompt on launch")
  - VAULT IDENTIFIER:** bullsequana\_edge\_password

CANCEL SAVE

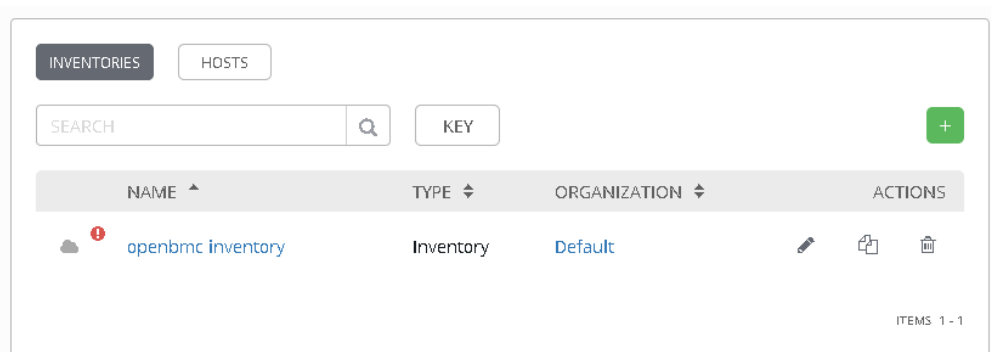
3. Complete the **Vault Password** field.
4. Click **Save**. The **Vault Password** field is now encrypted.

## 2.5.2. Creating an encrypted password for a host

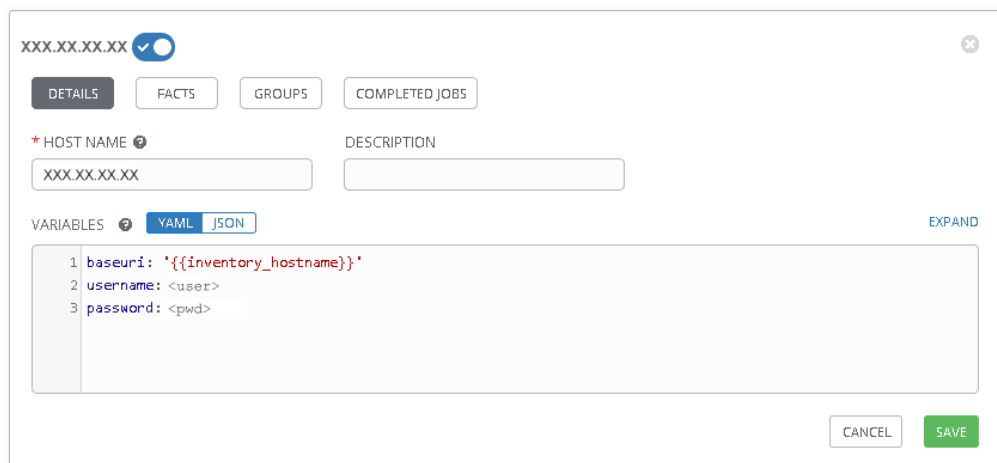
1. Choose a name for the password that is going to be encrypted.
2. Open a Terminal window.
3. Run the following command:

```
$ ./generate_encrypted_password_for_AWX.sh --name <password name> <host BMC password>
```

4. Enter the BullSequana Edge Vault password when asked. The encrypted password is generated.
5. From the left navigation bar, click **Inventories**. The **Inventories** page opens.



6. Click the inventory which contains the host to be edited. The inventory page opens.
7. Click **Hosts** and click the host to be edited. The host page opens.



8. Delete any previous passwords from the **Variables** field and add the following line.

```
password: '{{password name}}'
```

9. Click **Save**.



### 2.5.3. Deleting an encrypted password

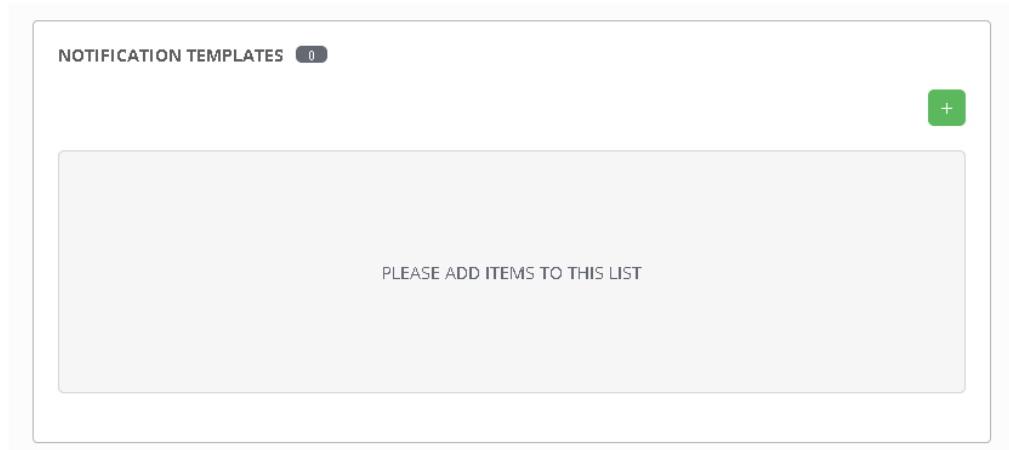
The encrypted passwords are stored in the `passwords.yml` file in the `/ansible/vars` sub-directory of the MISM installation directory. To delete one, perform the following actions:

1. Open the `passwords.yml` file in a text editor.
2. Locate the password to be deleted using the password name.
3. Delete the lines associated with the password.
4. Save and close the file.
5. Update the password in the host variables.

## 2.6. Setting up email alerts

### 2.6.1. Creating an email notification template

1. From the left navigation bar, click **Notifications**. The **Notifications** page opens.



2. Click the green +. A new page opens.
3. Complete the **Name** and the **organization** fields.
4. Select **Email** from the **Type** drop-down list.
5. Complete the fields as required.

## Example

The screenshot shows a 'NEW NOTIFICATION TEMPLATE' form with the following fields and values:

- NAME:** MyEmail
- DESCRIPTION:** (empty)
- ORGANIZATION:** Bull
- TYPE:** Email
- TYPE DETAILS:**
  - USERNAME:** (empty)
  - PASSWORD:** SHOW
  - HOST:** XXX.XX.XX.XX
  - RECIPIENT LIST:** YY.YY@atos.net
  - SENDER EMAIL:** XX.XX@atos.net
  - PORT:** 25
  - TIMEOUT:** 30
  - OPTIONS:** USE TLS (selected), USE SSL (unselected)
- CUSTOMIZE MESSAGES:** (toggle off)

Buttons: CANCEL, SAVE

**Important** TLS and SSL options are mutually exclusive. Be sure to only select one option. Checking both causes the notification to fail with no warning message.

- Click **Save** to complete changes.  
The notification template is created.

The screenshot shows a 'NOTIFICATION TEMPLATES' list with the following details:

- SEARCH:** (empty)
- KEY:** (empty)
- TABLE:**

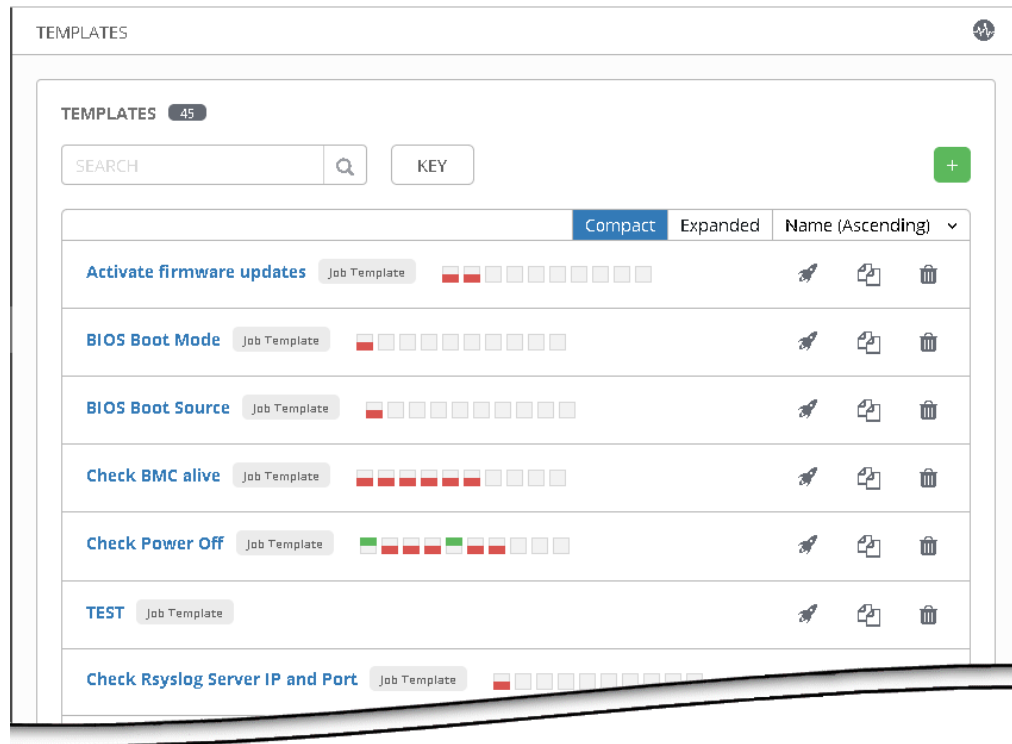
NAME	TYPE	ACTIONS
MyEmail	Email	
- ITEMS:** 1 - 1

- Click the test notification button to send a test email.

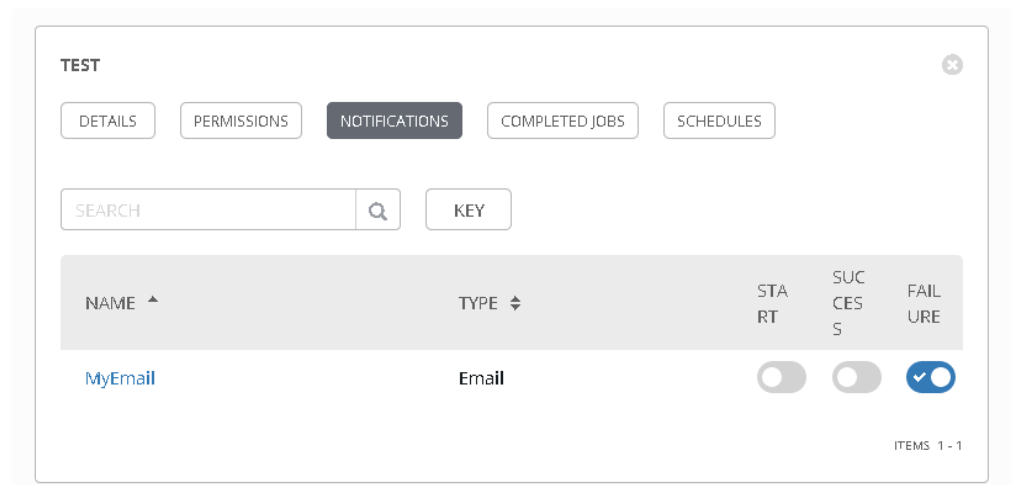
## 2.6.2. Assigning a notification to a job template

1. From the left navigation bar, click a resource (Templates, Projects or Inventories). A new page opens.

### Templates example



2. Click a resource.
3. Click the **Notifications** tab.



4. Use the toggle buttons to enable or disable the events.

## 2.7. Performing basic operations

### 2.7.1. Performing power operations

---

**Important** The https protocol must always be used to connect to the MISM console.

---

#### Powering servers on

1. Launch the **Power On** job.
2. Check that the job status is **Successful**.  
If the job status is **Failed**, check the output of the job in the text window.
3. Launch the **Check Power On** job.
4. Check that the job status is **Successful**.  
If the job status is **Failed**, check the output of the job in the text window.

#### W087 WARNING

**W087:**  
The Cold reboot and Immediate shutdown buttons should only be used if the Operating System is unable to respond to a Warm reboot or Orderly shutdown request.  
These sequences may result in data loss and file corruption.

#### Powering servers off

1. Select the power operation:
  - **Orderly Shutdown**
  - **Immediate Shutdown**
2. Launch the selected job.
3. Check that the job status is **Successful**.  
If the job status is **Failed**, check the output of the job in the text window.
4. Launch the **Check Power Off** job.
5. Check that the job status is **Successful**.  
If the job status is **Failed**, check the output of the job in the text window.

#### Rebooting BMC

1. Launch the **Reboot bmc** job.
2. Check that the job status is **Successful**.  
If the job status is **Failed**, check the output of the job in the text window.
3. Launch the **Check BMC alive** job.
4. Check that the job status is **Successful**.  
If the job status is **Failed**, check the output of the job in the text window.

## 2.7.2. Updating firmware

---

**Important**

- The BMC must be rebooted after an update of its firmware. If the reboot variable is set as False, it must be done manually for the update to be effective.
  - The host must be powered off before updating the BIOS or CPLD firmware. If the forceoff variable is set as False, it must be done manually.
- 

### 2.7.2.1. Updating firmware globally

#### Two-step operation

##### 1. Review which firmware will be updated

1. Launch the **Evaluate firmware update from Technical State** job.

---

**Note** The path to the Technical State file must be indicated as an inventory variable or as a job extra variable.

---

2. Check that the job is **Successful**.

If the job status is **Failed**, check the output of the job in the text window.

##### 2. Update the firmware

1. Launch the **Update firmware from Technical State** job.

---

**Note** The following variables must be indicated as inventory variables or as job extra variables:

- technical\_state\_path
  - reboot
  - forceoff
- 

2. Check that the job is **Successful**.

If the job status is **Failed**, check the output of the job in the text window.

3. Launch the **Firmware inventory - Active** job to get firmware versions.

4. Check that the job is **Successful**.

If the job status is **Failed**, check the output of the job in the text window.

#### Three-step operation

##### 1. Review which firmware will be updated

1. Launch the **Evaluate firmware update from Technical State** job to know which firmware will be updated.

---

**Note** The path to the Technical State file must be indicated as an inventory variable or as a job extra variable.

---

2. Check that the job is **Successful**.

If the job status is **Failed**, check the output of the job in the text window.

## 2. Upload the firmware

1. Launch the **Upload firmware images from Technical State** job.

---

**Note** The path to the Technical State file must be indicated as an inventory variable or as a job extra variable.

---

2. Check that the job is **Successful**.

If the job status is **Failed**, check the output of the job in the text window.

3. Launch the **Firmware inventory - Ready** job to get firmware versions.

4. Check that the job is **Successful**.

If the job status is **Failed**, check the output of the job in the text window.

## 3. Activate the firmware

1. Launch the **Activate firmware updates** job.

---

**Note** The following variables must be indicated as inventory variables or as job extra variables:

- reboot
  - forceoff
- 

2. Check that the job is **Successful**.

If the job status is **Failed**, check the output of the job in the text window.

3. Launch the **Firmware inventory - Active** job to get firmware versions.

4. Check that the job is **Successful**.

If the job status is **Failed**, check the output of the job in the text window.

### 2.7.2.2. Updating firmware individually

1. Launch the **Update firmware from file** job.

---

**Note** The following variables must be indicated as inventory variables or as job extra variables:

- reboot
  - forceoff
  - file\_to\_update
- 

2. Check that the job is **Successful**.

If the job status is **Failed**, check the output of the job in the text window.

3. Launch the **Firmware inventory - Active** job to get firmware versions.

4. Check that the job is **Successful**.

If the job status is **Failed**, check the output of the job in the text window.

## 2.7.3. Enabling syslog forwarding

### Prerequisites

The syslog server is configured for messaging

### Procedure

1. Indicate the syslog server IP address and port as variables in the inventory.

The screenshot shows the 'My first inventory' configuration page. At the top, there are tabs for DETAILS, PERMISSIONS, GROUPS, HOSTS, SOURCES, and COMPLETED JOBS. Below these are input fields for NAME (My first inventory), DESCRIPTION, ORGANIZATION (Default), INSIGHTS CREDENTIAL, and INSTANCE GROUPS. At the bottom, there is a VARIABLES section with a text editor showing the following YAML configuration:

```
1 forceoff: true
2 reboot: true
3
4 rsyslog_server_ip: <IP address>
5 rsyslog_server_port: <port number>
6
```

Buttons for CANCEL and SAVE are located at the bottom right of the interface.

2. Launch the **Set Rsyslog Server IP** job.
3. Check that the job is **Successful**.  
If the job status is **Failed**, check the output of the job in the text window.
4. Launch the **Set Rsyslog Server Port** job.
5. Check that the job is **Successful**.  
If the job status is **Failed**, check the output of the job in the text window.
6. Launch the **Check Rsyslog Server IP and Port** job to check the syslog server parameters.
7. Check that the job is **Successful**.  
If the job status is **Failed**, check the output of the job in the text window.



---

## Chapter 3. Monitoring resources

To monitor systems, the Machine Intelligence System Management (MISM) console uses Zabbix. Zabbix is an enterprise-class open source distributed monitoring solution accessible via a web-based interface.

---

**Important** Consult the full Zabbix documentation before using the MISM console:

<https://www.zabbix.com/documentation/current/manual>

---

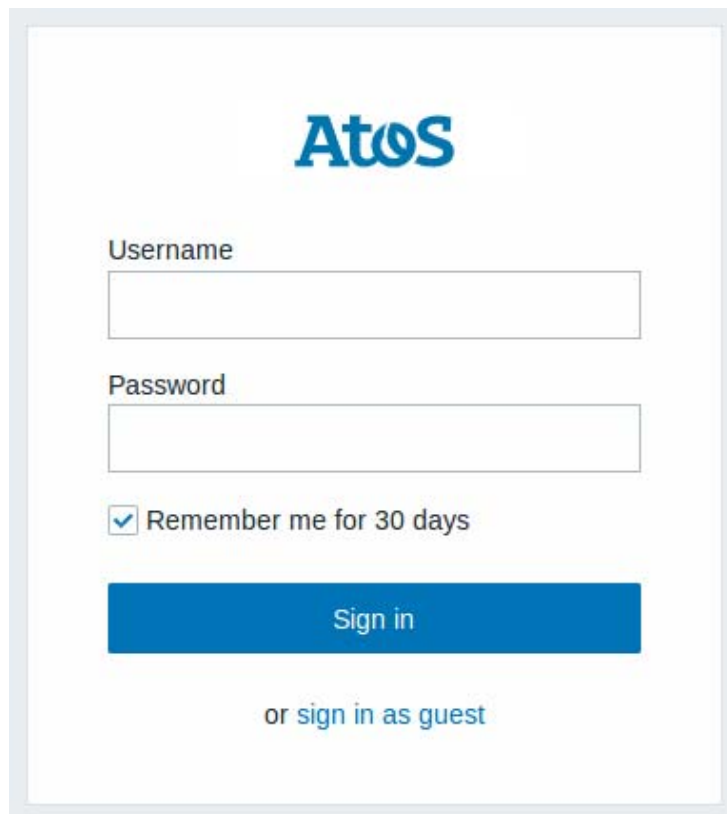
## 3.1. Logging in

### Procedure

1. Launch the web browser and enter the name or IP address of the MISM console followed by the port number 4443 using the https protocol:

**https://<IP address>:4443**

The authentication page opens.



Monitoring console	
Username	Default name: Admin
Password	Default password: zabbix

2. Complete the **Username** and **Password** fields and click **Sign in**. The **Dashboard** page opens.

### What to do if an incident occurs?

If the connection to the MISM 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)

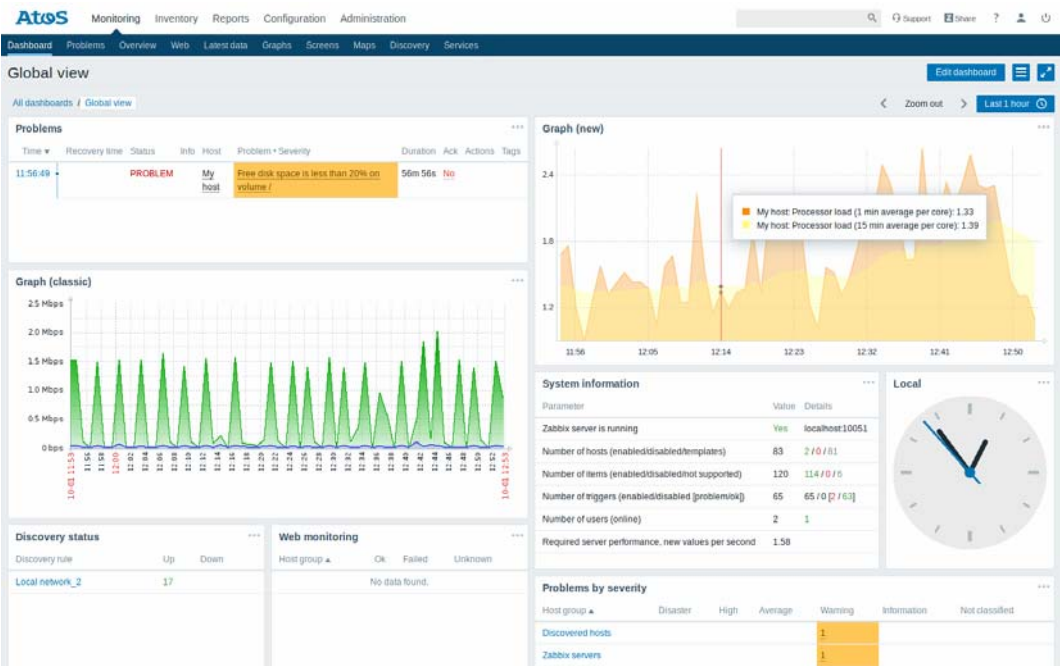
---

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

---

## 3.2. Console description

### 3.2.1. Console overview



Monitoring console description	
Menus	Five menus allow access to five families of features accessible from the associated tabs: Monitoring, Inventory, Reports, Configuration and Administration.
Tabs	Provides access to console features. Note that displayed features differ according to the selected menu.
Work pane	The work pane displays the information associated with the item selected in the menus.

## Features

Menu	Description	Features
Monitoring	Provides access to the information the monitoring console is configured to gather, visualize and act upon.	Dashboard
		Problems
		Overview
		Web
		Latest data
		Graphs
		Screens
		Maps
		Discovery
		Services
Inventory	Provides access to host inventory details.	Overview
		Hosts
Reports	Provides access to predefined and user-customizable reports displaying system information, triggers and gathered data.	System information
		Availability report
		Triggers Top 100
		Audit
		Action log
		Notifications
Configuration	Allows to set up major functions: hosts and host groups, data gathering, data thresholds, sending problem notifications, creating data visualization and others.	Host groups
		Templates
		Hosts
		Maintenance
		Actions
		Event correlation
		Discovery
		Services
Administration	Provides access to administrative functions. This menu is available to Super Administrator users only.	General
		Proxies
		Authentication
		User Groups
		Users
		Media types
		Scripts
		Queue

### 3.2.2. Delivery content

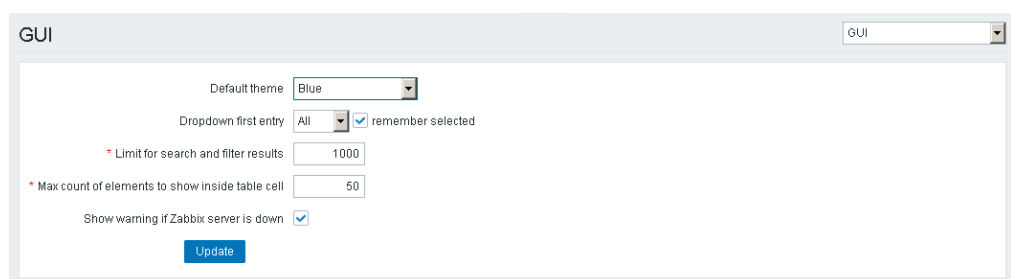
On delivery, the monitoring console contains two templates that allow Zabbix to be used to monitor BullSequana Edge servers:

- template-atos\_openbmc-lld-zbxv4.xml, containing all metrics, triggers and discovery items.
- template-atos\_openbmc-rsyslog-zbxv4.xml, containing the rsyslog info

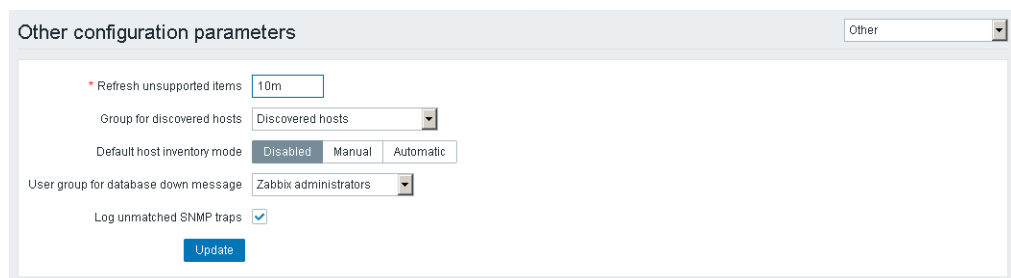
## 3.3. Preliminary configuration

### 3.3.1. Enabling automatic inventory

1. From the **Administration** menu, click the **General** tab. The **GUI** page opens.



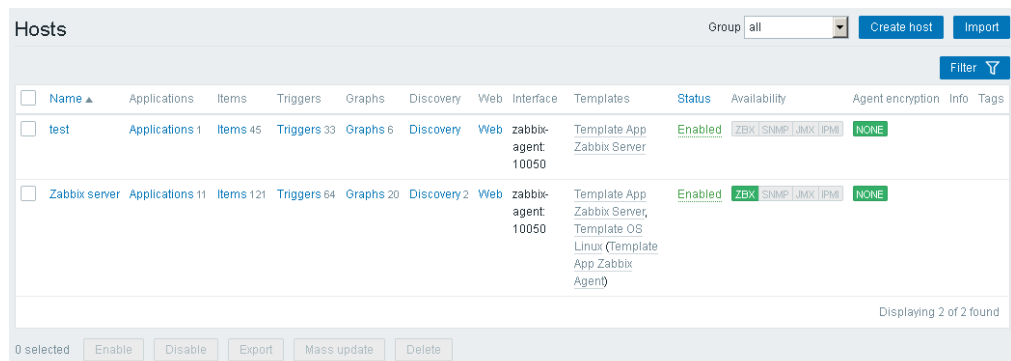
2. From the drop-down list on the right, click **Other**. The **Other configuration parameters** page opens.



3. Click **Automatic** for **Default host inventory mode**.
4. Click **Update**.

### 3.3.2. Renaming the Zabbix server host

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



Name	Applications	Items	Triggers	Graphs	Discovery	Web	Interface	Templates	Status	Availability	Agent encryption	Info	Tags
test	Applications 1	Items 45	Triggers 33	Graphs 6	Discovery	Web	zabbix-agent 10050	Template App Zabbix Server	Enabled	ZBX   SNMP   JMX   IPMI	NONE		
Zabbix server	Applications 11	Items 121	Triggers 64	Graphs 20	Discovery 2	Web	zabbix-agent 10050	Template App Zabbix Server, Template OS Linux (Template App Zabbix Agent)	Enabled	ZBX   SNMP   JMX   IPMI	NONE		

- Click the **Zabbix server** line. The details of the host are displayed.

The screenshot shows the Zabbix web interface for configuring a host. The host name is 'zabbix-server' and the visible name is 'Zabbix server'. The group is 'Zabbix servers'. The 'Agent interfaces' section shows a table with columns for IP address, DNS name, Connect to, Port, and Default. The 'DNS' tab is selected, and the 'zabbix-agent' is listed with port 10050. The 'Enabled' checkbox is checked.

- Complete the following fields.

Field	Value
Host name	zabbix-server
Visible name	Zabbix server

- In the **Agent interfaces** section, perform the following actions:
  - Click **DNS**.
  - Complete the following fields.

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

- Click **Update**.
- Stop and restart the MISM console.

## 3.4. Managing Atos LLD template

### 3.4.1. Template description

The template allows the following elements on the servers to be monitored:

- Fan, temperature and voltage information in Discovery applications
- Four discovered triggers:
  - Critical high and low triggers, corresponding to Critical Alarm Thresholds for BullSequana Edge servers, that are enabled by default
  - Warning high and low triggers, corresponding to Warning Alarm Thresholds for BullSequana Edge servers, that are disabled by default

### 3.4.2. Importing the Atos LLD template

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

The screenshot shows the Zabbix Templates page. At the top, there's a 'Group' dropdown set to 'all', and buttons for 'Create template' and 'Import'. Below this is a search bar for 'Name' and a 'Filter' icon. There are also fields for 'Linked templates' and 'Tags' with 'And/Or' and 'Or' options. A table of templates is displayed with columns: Name, Applications, Items, Triggers, Graphs, Screens, Discovery, and Webhooks. The table lists various templates like 'Template App Apache Tomcat JMX', 'Template App FTP Service', 'Template App Generic Java JMX', 'Template App HTTP Service', 'Template App HTTPS Service', 'Template App IMAP Service', 'Template App LDAP Service', 'Template App NNTP Service', 'Template App NTP Service', 'Template App POP Service', 'Template App Remote Zabbix proxy', 'Template App Remote Zabbix server', and 'Template Net Extreme EXOS SNMPv2'. At the bottom, there's a pagination bar showing '1 2' and a status 'Displaying 1 to 50 of 83 found'.

Name	Applications	Items	Triggers	Graphs	Screens	Discovery	Webhooks
Template App Apache Tomcat JMX	Applications 5	Items 32	Triggers 5	Graphs 4	Screens	Discovery	Webhooks
Template App FTP Service	Applications 1	Items 1	Triggers 1	Graphs	Screens	Discovery	Webhooks
Template App Generic Java JMX	Applications 8	Items 55	Triggers 26	Graphs 11	Screens	Discovery	Webhooks
Template App HTTP Service	Applications 1	Items 1	Triggers 1	Graphs	Screens	Discovery	Webhooks
Template App HTTPS Service	Applications 1	Items 1	Triggers 1	Graphs	Screens	Discovery	Webhooks
Template App IMAP Service	Applications 1	Items 1	Triggers 1	Graphs	Screens	Discovery	Webhooks
Template App LDAP Service	Applications 1	Items 1	Triggers 1	Graphs	Screens	Discovery	Webhooks
Template App NNTP Service	Applications 1	Items 1	Triggers 1	Graphs	Screens	Discovery	Webhooks
Template App NTP Service	Applications 1	Items 1	Triggers 1	Graphs	Screens	Discovery	Webhooks
Template App POP Service	Applications 1	Items 1	Triggers 1	Graphs	Screens	Discovery	Webhooks
Template App Remote Zabbix proxy	Applications 1	Items 32	Triggers 23	Graphs 4	Screens 1	Discovery	Webhooks
Template App Remote Zabbix server	Applications 1	Items 1	Triggers 1	Graphs	Screens	Discovery	Webhooks
Template Net Extreme EXOS SNMPv2	Applications 9	Items 19	Triggers 11	Graphs 1	Screens	Discovery 5	Webhooks

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

Rules	Update existing	Create new	Delete missing
Groups	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Hosts	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Templates	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Template screens	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Template linkage	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Applications	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Items	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Discovery rules	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Triggers	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Graphs	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Web scenarios	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Screens	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Maps	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Images	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Value mappings	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

3. In **Import file** section, click **Browse** and indicate the path to the template.

---

**Note** The templates are delivered in a sub-directory of the MISM intallation directory: \zabbix\server\externalscripts. They can be copied to any local directory.

---

4. Click **Import**.

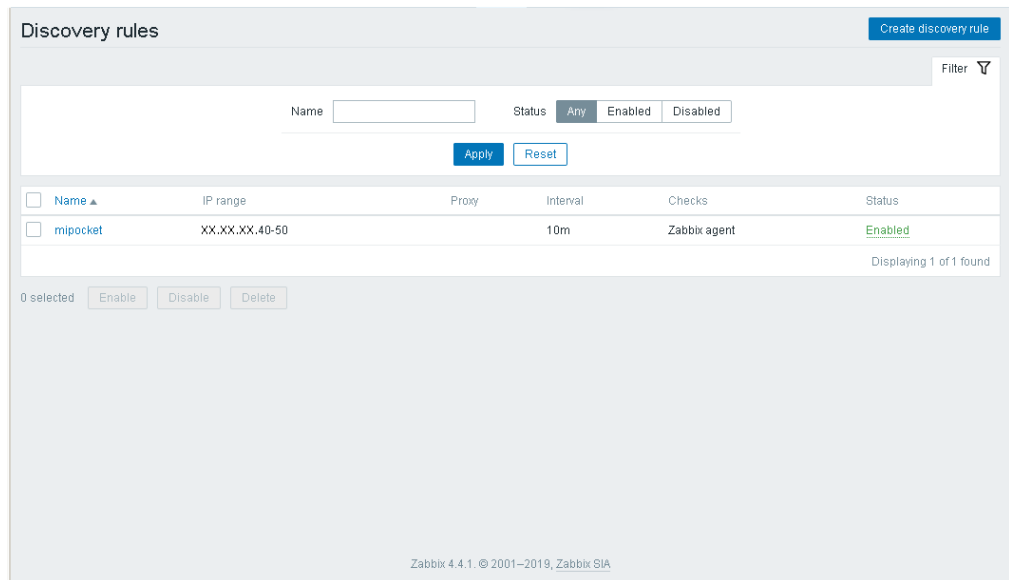


## 3.5. Adding resources

### 3.5.1. Adding hosts with the zabbix discovery service

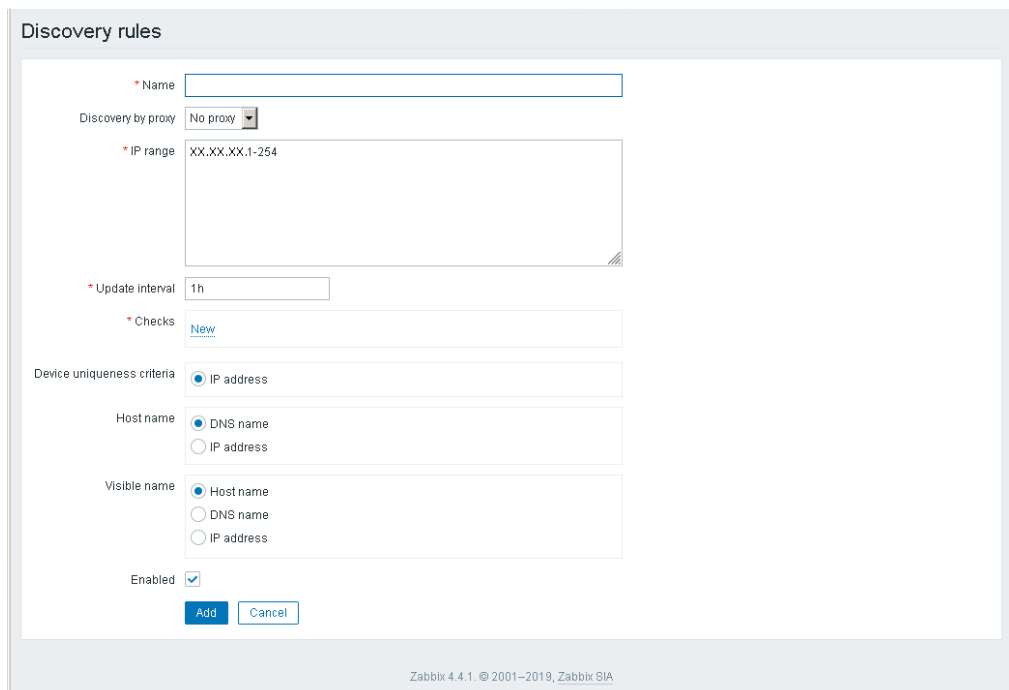
#### 3.5.1.1. Creating a discovery rule

1. From the **Configuration** menu, click the **Discovery** tab. The **Discovery rules** page opens.



The screenshot shows the 'Discovery rules' page in Zabbix. At the top right is a 'Create discovery rule' button. Below it is a search bar with a 'Filter' icon. The main area contains a table with columns: Name, IP range, Proxy, Interval, Checks, and Status. One rule is listed: 'mipocket' with IP range 'XX.XX.XX.40-50', interval '10m', checks 'Zabbix agent', and status 'Enabled'. Below the table are buttons for '0 selected', 'Enable', 'Disable', and 'Delete'. The footer shows 'Zabbix 4.4.1. © 2001–2019, Zabbix SIA'.

2. Click **Create discovery rule**. A new page opens.



The screenshot shows the 'Create discovery rule' page. It has several form fields: 'Name' (required), 'Discovery by proxy' (dropdown, currently 'No proxy'), 'IP range' (required, with a text area showing 'XX.XX.XX.1-254'), 'Update interval' (text field, currently '1h'), 'Checks' (text field, with a 'New' link), 'Device uniqueness criteria' (radio buttons, currently 'IP address'), 'Host name' (radio buttons, currently 'DNS name'), and 'Visible name' (radio buttons, currently 'Host name'). There is an 'Enabled' checkbox checked. At the bottom are 'Add' and 'Cancel' buttons. The footer shows 'Zabbix 4.4.1. © 2001–2019, Zabbix SIA'.

3. Complete the **Name** field.
4. Complete the **IP range** field.
5. Modify the **Update interval** (default value: 1h).

6. In the **Checks** section, perform the following actions:
  - a. Click **New**.
  - b. Select **HTTPS** from the **Check type** drop-down list.
  - c. Click **Add**.
7. Complete the **Host name** section as required.

### Example

The screenshot shows the 'Discovery rules' configuration form in Zabbix. The form includes the following fields and options:

- Name:** MyMipockets
- Discovery by proxy:** No proxy
- IP range:** XX.XX.X.1-254
- Update interval:** 10m
- Checks:**
  - [New](#)
  - Check type:** HTTPS
  - Port range:** 443
  - [Add](#) [Cancel](#)
- Device uniqueness criteria:** ☒ IP address
- Host name:** ☐ DNS name ☒ IP address
- Visible name:** ☐ Host name ☐ DNS name ☒ IP address
- Enabled:** ☒
- [Add](#) [Cancel](#)

Zabbix 4.4.1. © 2001–2019, Zabbix SIA

8. Click **Add** to complete changes.
- The discovery rule is created.

### Example

The screenshot shows the 'Discovery rules' list page in Zabbix. A notification at the top states 'Discovery rule created'. The table below lists the discovery rules:

Name	IP range	Proxy	Interval	Checks	Status
<input type="checkbox"/> mipocket	XX.XX.XX.40-50		10m	Zabbix agent	Enabled
<input type="checkbox"/> MyMipockets	XX.XX.X.1-254		10m	HTTPS	Enabled

0 selected [Enable](#) [Disable](#) [Delete](#)

Displaying 2 of 2 found

Zabbix 4.4.1. © 2001–2019, Zabbix SIA

### 3.5.1.2. Creating an action linked to the discovery rule

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

Actions

Event source: **Discovery** [Create action](#)

Filter

Name  Status: **Any** Enabled Disabled [Apply](#) [Reset](#)

<input type="checkbox"/> Name	Conditions	Operations	Status
<input type="checkbox"/> <a href="#">Auto discovery: Linux servers</a>	Received value contains <i>Linux</i> Discovery status equals <i>Up</i> Service type equals <i>Zabbix agent</i> Host IP equals <i>XX.XX.XX.1-127.XX.XX.XX.1</i>	<b>Add host</b> <b>Add to host groups:</b> Linux servers <b>Link to templates:</b> Template Hw Atos BullSequanaEdge LLD <b>Enable host</b> <b>Set host inventory mode:</b> Automatic	Disabled
<input type="checkbox"/> <a href="#">mipocket discover</a>	Discovery rule equals <i>mipocket</i>	<b>Add host</b>	Enabled

0 selected [Enable](#) [Disable](#) [Delete](#) Displaying 2 of 2 found

Zabbix 4.4.1. © 2001–2019, Zabbix SIA

2. From the **Event source** drop-down list, select **Discovery**.
3. Click the **Create action** button. A new page opens.

Actions

**Action** **Operations**

\* Name

Conditions

Label	Name	Action
New condition	Host IP	equals

[Add](#)

Enabled ☒

\* At least one operation must exist.

[Add](#) [Cancel](#)

Zabbix 4.4.1. © 2001–2019, Zabbix SIA

4. Complete the **Name** field.
  5. Add a new condition.
- In the **New condition** section, perform the following actions:
- a. Select **Discovery rule** and **equals** from the drop-down lists.
  - b. Click **Select**.
  - c. Select the discovery rule previously created.
  - d. Click **Add**.

## Example

Actions

Action Operations

\* Name

Conditions

Label	Name	Action
-------	------	--------

New condition

Discovery rule equals MyMipockets

Select

Add

Enabled ☒

\* At least one operation must exist.

Add Cancel

Zabbix 4.4.1. © 2001–2019, Zabbix SIA

## 4. Configure the operations

1. Click the **Operations** tab.

Actions

Action Operations

Default subject

Discovery: (DISCOVERYDEVICE.STATUS) (DISCOVERYDEVICE.IPADDRESS)

Default message

Discovery rule: (DISCOVERYRULE.NAME)

Device IP: (DISCOVERYDEVICE.IPADDRESS)

Device DNS: (DISCOVERYDEVICE.DNS)

Device status: (DISCOVERYDEVICE.STATUS)

Device uptime: (DISCOVERYDEVICE.uptime)

Device service name: (DISCOVERYSERVICE.NAME)

Operations

Details	Action
---------	--------

\* At least one operation must exist.

Add Cancel

Zabbix 4.4.1. © 2001–2019, Zabbix SIA

2. Add the operations.

For each required operation, perform the following steps:

- a. In the **Operations** section, click **New**.
- b. In the **Operation details** section, perform the following actions:
  - i. From the **Operation type** drop-down list, select an operation.
  - ii. Click **Add**.

## Example

**Actions**

Default subject: Discovery: {DISCOVERYDEVICE.STATUS} {DISCOVERYDEVICE.IPADDRESS}

Default message:

```
Discovery rule: {DISCOVERYRULE.NAME}
Device IP: {DISCOVERYDEVICE.IPADDRESS}
Device DNS: {DISCOVERYDEVICE.DNS}
Device status: {DISCOVERYDEVICE.STATUS}
Device uptime: {DISCOVERYDEVICE.uptime}
Device service name: {DISCOVERYSERVICE.NAME}
```

Operations:

Details	Action
<b>Add host</b>	<a href="#">Edit</a> <a href="#">Remove</a>
<b>Add to host groups:</b> Discovered hosts	<a href="#">Edit</a> <a href="#">Remove</a>
<b>Link to templates:</b> Template Hw Atos BullSequanaEdge LLD	<a href="#">Edit</a> <a href="#">Remove</a>
<b>Enable host</b>	<a href="#">Edit</a> <a href="#">Remove</a>

Operation details:

Operation type: Set host inventory mode

Inventory mode: ☐ Manual ☒ Automatic

[Add](#) [Cancel](#)

\* At least one operation must exist.

[Update](#) [Clone](#) [Delete](#) [Cancel](#)

**Important** When the Discovery action has been configured and enabled, it may later be disabled to prevent continuous host discovery and also to allow changes to be made to hosts.

3. Save the action.
- Click **Add** to complete changes.

## Example

✓ Action added

Event source: Discovery [Create action](#)

Filter

Name:  Status: ☒ Any ☐ Enabled ☐ Disabled [Apply](#) [Reset](#)

<input type="checkbox"/> Name	Conditions	Operations	Status
<input type="checkbox"/> Auto discovery: Linux servers.	Received value contains Linux Discovery status equals Up Service type equals Zabbix agent Host IP equals XX.XX.XX.1-127, XX.XX.XX.1	<b>Add host</b> <b>Add to host groups:</b> Linux servers <b>Link to templates:</b> Template Hw Atos BullSequanaEdge LLD <b>Enable host</b> <b>Set host inventory mode:</b> Automatic	Disabled
<input type="checkbox"/> discover mipocket action	Discovery rule equals MyMipockets	<b>Add host</b> <b>Add to host groups:</b> Discovered hosts <b>Link to templates:</b> Template Hw Atos BullSequanaEdge LLD <b>Enable host</b> <b>Set host inventory mode:</b> Automatic	Enabled
<input type="checkbox"/> mipocket discover	Discovery rule equals mipocket	<b>Add host</b>	Enabled

0 selected [Enable](#) [Disable](#) [Delete](#)

Displaying 3 of 3 found

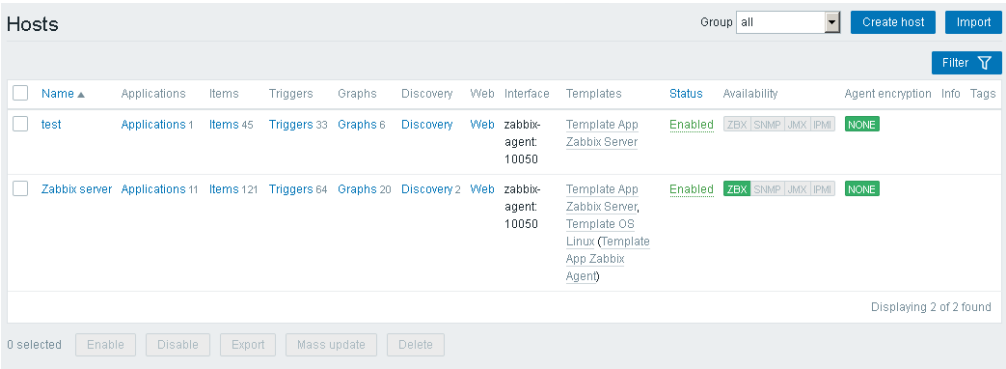
<https://172.31.131.101:4443/zabbix.php?action=dashboard.view>

4. Complete the hosts with { \$OPENBMC }, { \$USER }, { \$PASSWORD }.

**See** 3.5.4. Filling Atos template macros

### 3.5.2. Adding a host manually

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



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

3. Complete the **Host name** with the host BMC IP address.
4. In the **Groups** section, click **Select** and select **Zabbix servers**.
5. In the **Agent interfaces** section, perform the following actions:
  - a. Click **DNS**.
  - b. Complete the following fields.

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

6. Click **Add**.

### 3.5.3. Linking a host to the Atos LLD template

1. From the **Hosts** page, click on the newly created host. The host details are displayed.

The screenshot shows the Zabbix Host configuration page for a host named 'test'. The page has tabs for Host, Templates, IPMI, Tags, Macros, Inventory, and Encryption. The Host tab is active. The configuration includes fields for Host name (test), Visible name, and Groups (Zabbix servers). A note states 'At least one interface must exist.' Below this, there are sections for Agent interfaces, SNMP interfaces, JMX interfaces, and IPMI interfaces. The Agent interfaces section shows a table with columns for IP address, DNS name (zabbix-agent), Connect to (IP/DNS), Port (10050), and Default (selected). There are 'Add' and 'Remove' buttons. Below the interface sections is a Description text area, a 'Monitored by proxy' dropdown (set to 'no proxy'), and an 'Enabled' checkbox (checked). At the bottom are buttons for Update, Clone, Full clone, Delete, and Cancel.

2. Click the **Template** tab above the host details. The host Template page opens.

The screenshot shows the Zabbix Host Template configuration page for the same host 'test'. The Templates tab is active. It displays 'Linked templates' with a table showing 'Template App Zabbix Server' and actions 'Unlink' and 'Unlink and clear'. Below this is the 'Link new templates' section with a search input and a 'Select' button. An 'Add' button is also present. At the bottom are buttons for Update, Clone, Full clone, Delete, and Cancel.

3. In the **Link new templates** section, click **Select** and select the Atos LLD template.
4. Click **Add**. The Atos LLD template appears in the **Linked templates** section.
5. Click **Update**.

### 3.5.4. Filling Atos template macros

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

For each BullSequana Edge host, repeat the steps:

2. Click a host **Name**.
3. Click the **Macros** tab.

4. Add the Password, User and OpenBMC macros.

Macro	Value
{ \$PASSWORD }	Host OpenBMC password
{ \$USER }	Host OpenBMC username
{ \$OPENBMC }	Host BMC address

For each macro:

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



## Example

The screenshot shows the Zabbix web interface for editing a host's macros. The breadcrumb trail is: All hosts / 172.31.130.34 / Enabled / ZBX / SNMP / JMX / IPMI. The 'Macros' tab is selected, showing a table of macros. The table has three columns: Macro, Value, and Description. There are three macros listed: (\$OPENBMC) with value XX.XX.XX.XX, (\$PASSWORD) with value mypassword@atos, and (\$USER) with value root. Each macro has a 'Remove' link. Below the table are buttons for 'Add', 'Update', 'Clone', 'Full clone', 'Delete', and 'Cancel'. The footer text is 'Zabbix 4.4.1. © 2001–2019, Zabbix SIA'.

Macro	Value	Description
(\$OPENBMC)	XX.XX.XX.XX	description
(\$PASSWORD)	mypassword@atos	description
(\$USER)	root	description

[Add](#) [Update](#) [Clone](#) [Full clone](#) [Delete](#) [Cancel](#)

Zabbix 4.4.1. © 2001–2019, Zabbix SIA

---

**See** 3.6. Adding security if an encrypted password is necessary.

---

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

## 3.6. Adding security

### 3.6.1. Activating PSK security

1. Open a Terminal window.
2. Go the MISM installation directory.
3. Generate an encryption key using the following command:

```
$ generate_psk_key_for_zabbix.sh
```

The `zabbix_agentd.psk` file, containing the key, is generated in the `/etc/zabbix/agent/` directory.

4. Go to the `/etc/zabbix/agent/` directory and open the `zabbix_agentd.conf` file with a text editor.
5. In the `TLS-RELATED PARAMETERS` section of the file, uncomment the following lines:

```
-----
TLSConnect=psk
TLSAccept=psk
TLSPSKIdentity=PSK_Mipocket_Agent
TLSPSKFile=/etc/zabbix/zabbix_agentd.psk
-----
```

6. Save and close the file.
7. Stop and restart the MISM console.

### 3.6.2. Enabling PSK security for a host

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

<input type="checkbox"/>	Name ▲	Applications	Items	Triggers	Graphs	Discovery	Web	Interface	Templates	Status	Availability	Agent encryption	Info	Tags
<input type="checkbox"/>	test	Applications 1	Items 45	Triggers 33	Graphs 6	Discovery	Web	zabbix-agent 10050	Template App Zabbix Server	Enabled	ZBX SNMP JMX IPMI	NONE		
<input type="checkbox"/>	Zabbix server	Applications 11	Items 121	Triggers 64	Graphs 20	Discovery 2	Web	zabbix-agent 10050	Template App Zabbix Server, Template OS Linux (Template App Zabbix Agent)	Enabled	ZBX SNMP JMX IPMI	NONE		

0 selected   Enable   Disable   Export   Mass update   Delete

Displaying 2 of 2 found

- Click on the host. The host details are displayed.

The screenshot shows the Zabbix web interface for configuring a host named 'test'. The 'Host' tab is selected. Fields include 'Host name' (test), 'Visible name', 'Groups' (Zabbix servers), and 'Agent interfaces' (IP address, DNS name: zabbix-agent, Connect to: IP, Port: 10050). There are also sections for SNMP, JMX, and IPMI interfaces, a description field, and a 'Monitored by proxy' dropdown. At the bottom, there are buttons for 'Update', 'Clone', 'Full clone', 'Delete', and 'Cancel'.

- Click the **Encryption** tab above the host details. The host Encryption page opens.

The screenshot shows the 'Encryption' tab for the host 'test'. It has two sections: 'Connections to host' with tabs for 'No encryption', 'PSK', and 'Certificate'; and 'Connections from host' with checkboxes for 'No encryption' (checked), 'PSK', and 'Certificate'. At the bottom are buttons for 'Update', 'Clone', 'Full clone', 'Delete', and 'Cancel'.

- In the Connections to host section, click PSK.
- In the Connections from host, select PSK.
- Complete the following fields.

Field	Value
PSK Identity	PSK_Mipocket_Agent
echo PSK	Encryption key from the zabbix_agentd.psk file

- Click **Update**.
- Stop and restart the MISM console.

### 3.6.3. Creating an encrypted password for a host

- Go the MISM installation directory.
- Generate an encrypted password using the following command:

```
$ generate_encrypted_password_for_zabbix.sh --password=<host BMC password>
```

- Copy the encrypted password.

4. From the **Configuration** menu, click the **Hosts** tab. The **Hosts** page opens.

Name	Applications	Items	Triggers	Graphs	Discovery	Web	Interface	Templates	Status	Availability	Agent encryption	Info	Tags
test	Applications 1	Items 45	Triggers 33	Graphs 6	Discovery	Web	zabbix-agent 10050	Template App Zabbix Server	Enabled	ZBX   SNMP   JMX   IPMI	NONE		
Zabbix server	Applications 11	Items 121	Triggers 64	Graphs 20	Discovery 2	Web	zabbix-agent 10050	Template App Zabbix Server, Template OS Linux (Template App Zabbix Agent)	Enabled	ZBX   SNMP   JMX   IPMI	NONE		

5. Click the host. The host details are displayed.

Host details for 'test'.

Host name: test

Visible name:

Groups: Zabbix servers

Agent interfaces:

IP address	DNS name	Connect to	Port	Default
	zabbix-agent	IP	10050	<input checked="" type="radio"/> Remove

SNMP interfaces: Add

JMX interfaces: Add

IPMI interfaces: Add

Description:

Monitored by proxy: (no proxy)

Enabled: ☒

Buttons: Update, Clone, Full clone, Delete, Cancel

6. Click the **Macros** tab above the host details. The host Macros page opens.

Host macros for 'test'.

Macro	Value
{PASSWORD}	value

Buttons: Update, Clone, Full clone, Delete, Cancel

7. Paste the encrypted password in the **Value** field of the **{PASSWORD}** macro.
8. Click **Update**.

## 3.7. Enabling syslog forwarding

### 3.7.1. Importing the Atos Rsyslog template

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

The screenshot shows the 'Templates' page. At the top, there's a 'Group' dropdown set to 'all', and buttons for 'Create template' and 'Import'. Below this is a search section with a 'Name' input field, a 'Linked templates' search box, and a 'Tags' section with 'And/Or' and 'Or' radio buttons, and a 'tag' input field. There are also 'Contains', 'Equals', and 'value' buttons. Below the search section is a table of templates. The table has columns for 'Name', 'Applications', 'Items', 'Triggers', 'Graphs', 'Screens', 'Discovery', and 'Web'. The table lists various templates like 'Template App Apache Tomcat JMX', 'Template App FTP Service', etc. At the bottom, there's a pagination bar showing '1 2' and 'Displaying 1 to 50 of 83 found'.

Name	Applications	Items	Triggers	Graphs	Screens	Discovery	Web
Template App Apache Tomcat JMX	Applications 5	Items 32	Triggers 5	Graphs 4	Screens	Discovery	Web
Template App FTP Service	Applications 1	Items 1	Triggers 1	Graphs	Screens	Discovery	Web
Template App Generic Java JMX	Applications 8	Items 55	Triggers 26	Graphs 11	Screens	Discovery	Web
Template App HTTP Service	Applications 1	Items 1	Triggers 1	Graphs	Screens	Discovery	Web
Template App HTTPS Service	Applications 1	Items 1	Triggers 1	Graphs	Screens	Discovery	Web
Template App IMAP Service	Applications 1	Items 1	Triggers 1	Graphs	Screens	Discovery	Web
Template App LDAP Service	Applications 1	Items 1	Triggers 1	Graphs	Screens	Discovery	Web
Template App NNTP Service	Applications 1	Items 1	Triggers 1	Graphs	Screens	Discovery	Web
Template App NTP Service	Applications 1	Items 1	Triggers 1	Graphs	Screens	Discovery	Web
Template App POP Service	Applications 1	Items 1	Triggers 1	Graphs	Screens	Discovery	Web
Template App Remote Zabbix proxy	Applications 1	Items 32	Triggers 23	Graphs 4	Screens 1	Discovery	Web
Template App Remote Zabbix server	Applications 1	Items 32	Triggers 23	Graphs 4	Screens 1	Discovery	Web
Template Net Extreme EXOS SNMPv2	Applications 9	Items 19	Triggers 11	Graphs 1	Screens	Discovery 5	Web

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

The screenshot shows the 'Import' page. At the top, there's a section for 'Import file' with a 'Parcourir...' button and the text 'Aucun fichier sélectionné.' Below this is a 'Rules' section with a table of checkboxes for different components. The table has columns for 'Update existing', 'Create new', and 'Delete missing'. The components listed are Groups, Hosts, Templates, Template screens, Template linkage, Applications, Items, Discovery rules, Triggers, Graphs, Web scenarios, Screens, Maps, Images, and Value mappings. At the bottom, there are 'Import' and 'Cancel' buttons.

Rules	Update existing	Create new	Delete missing
Groups	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Hosts	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Templates	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Template screens	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Template linkage	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Applications	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Items	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Discovery rules	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Triggers	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Graphs	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Web scenarios	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Screens	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Maps	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Images	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Value mappings	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

3. In the **Import file** section, click **Browse** and indicate the path to the template.

---

**Note** The templates are delivered in a sub-directory of the MISM installation directory: \zabbix\server\externalscripts. They can be copied to any local directory.

---

4. Click **Import**.

### 3.7.2. Linking the Zabbix server host to the Atos Rsyslog template

1. From the **Hosts** page, click on Zabbix server host. The host details are displayed.

The screenshot shows the Zabbix web interface for editing a host named 'zabbix-server'. The breadcrumb trail is 'All hosts / Zabbix server'. The status is 'Enabled' with tabs for 'ZBX', 'SNMP', 'JMX', and 'IPMI'. Navigation links include 'Applications 11', 'Items 121', 'Triggers 64', 'Graphs 20', 'Discovery rules 2', and 'Web scenarios'. The 'Host' tab is active, showing fields for 'Host name' (zabbix-server), 'Visible name' (Zabbix server), and 'Groups' (Zabbix servers). A note states '\* At least one interface must exist.' Below this are sections for 'Agent interfaces', 'SNMP interfaces', 'JMX interfaces', and 'IPMI interfaces', each with an 'Add' button. The 'Agent interfaces' section shows a table with columns for IP address, DNS name (zabbix-agent), Connect to (IP/DNS), Port (10050), and a 'Default' checkbox. At the bottom, there is a 'Description' text area, a 'Monitored by proxy' dropdown (set to 'no proxy'), an 'Enabled' checkbox, and buttons for 'Update', 'Clone', 'Full clone', 'Delete', and 'Cancel'.

2. Click the **Template** tab above the host details. The host Template page opens.

The screenshot shows the 'Template' tab in the Zabbix web interface for the 'zabbix-server' host. The breadcrumb trail is 'All hosts / Zabbix server'. The status is 'Enabled' with tabs for 'ZBX', 'SNMP', 'JMX', and 'IPMI'. Navigation links are the same as the previous screenshot. The 'Template' tab is active, showing a table of 'Linked templates' with columns for 'Name' and 'Action'. The linked templates are 'Template App Zabbix Server' and 'Template OS Linux'. Below this is a 'Link new templates' section with a search input and a 'Select' button. At the bottom, there are buttons for 'Update', 'Clone', 'Full clone', 'Delete', and 'Cancel'.

3. In the **Link new templates** section, click **Select** and select the Atos Rsyslog template.
4. Click **Add**. The Atos Rsyslog template appears in the **Linked templates** section.
5. Click **Update**.

### 3.7.3. Displaying the logs

1. From the **Monitoring** menu, click the Dashboard tab. The last selected dashboard opens.
2. If the displayed dashboard is not the Rsyslog dashboard, click **All dashboards** and click Rsyslog dashboard in the dashboard list.

## 3.8. Configuring nmap

### 3.8.1. Creating a nmap discovery rule

1. From the **Configuration** menu, click the **Discovery** tab. The **Discovery rules** page opens.

Discovery rules

Create discovery rule

Filter

Name  Status Any Enabled Disabled

Apply Reset

<input type="checkbox"/>	Name	IP range	Proxy	Interval	Checks	Status
<input type="checkbox"/>	mipocket	XXX.XXX.XX.XX 40-50		10m	Zabbix agent	Enabled

0 selected Enable Disable Delete

Displaying 1 of 1 found

Zabbix 4.4.1. © 2001–2019, Zabbix SIA

2. Click the **Create Discovery rule** button. A new page opens.

Discovery rules

\* Name

Discovery by proxy No proxy

\* IP range

\* Update interval

\* Checks [New](#)

Device uniqueness criteria ☒ IP address

Host name ☒ DNS name ☐ IP address

Visible name ☒ Host name ☐ DNS name ☐ IP address

Enabled ☒

Add Cancel

Zabbix 4.4.1. © 2001–2019, Zabbix SIA

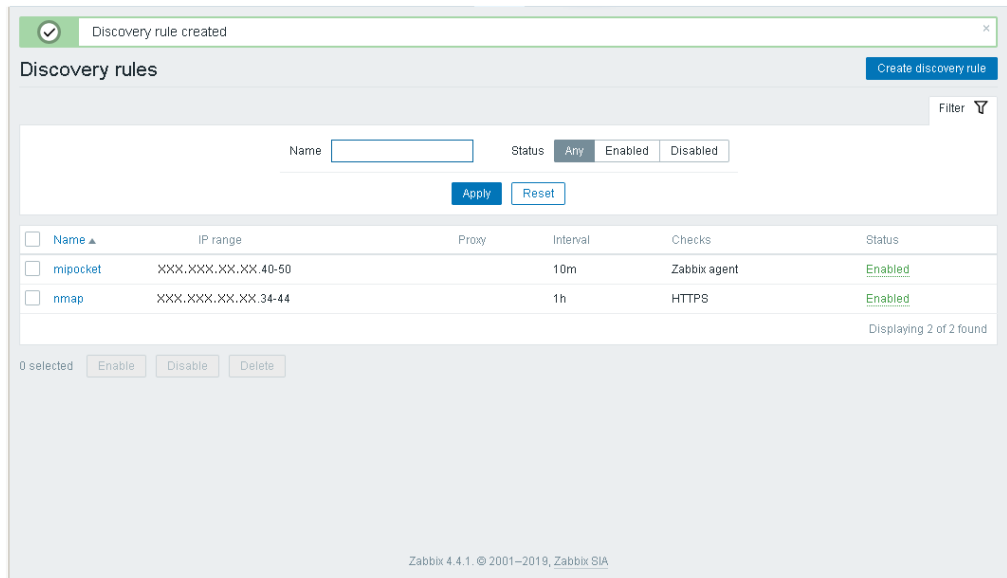
3. Complete the **Name** and **IP range** fields.
4. Configure the check type.

In the **Checks** section, click **New** and perform the following actions:

- a. From the **Check type** drop-down list, select **HTTPS**.
- b. Click **Add**.



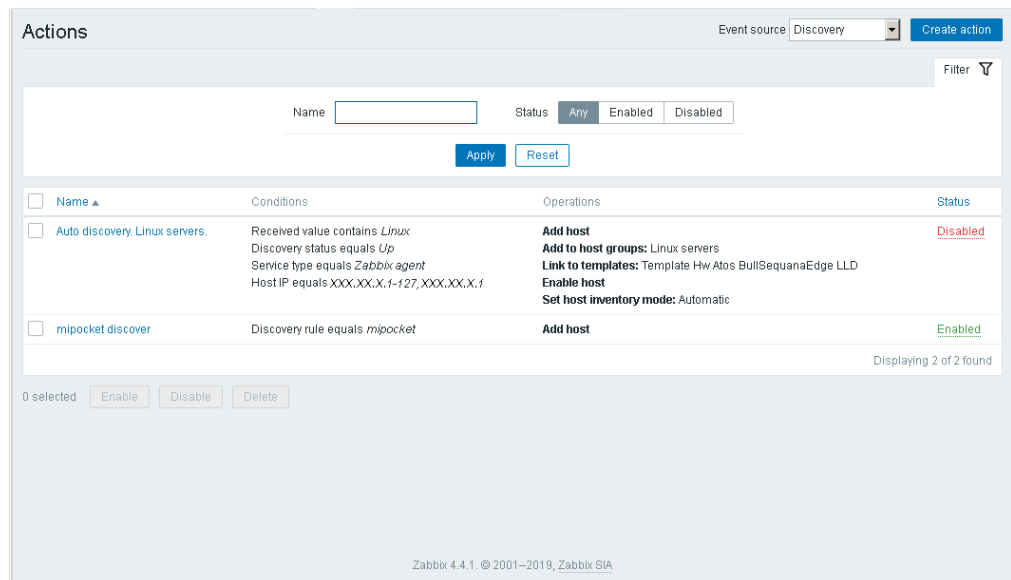
5. Save the discovery rule.
- Click **Add** to complete changes.
- The nmap discovery rule is created.



### 3.8.2. Creating a nmap action

#### 1. Configure a new action

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



2. From the **Event source** drop-down list, select **Discovery**.

3. Click the **Create action** button. A new page opens.

The screenshot shows the 'Actions' configuration page in Zabbix, specifically the 'Operations' tab. The page has a header 'Actions' and two sub-tabs: 'Action' and 'Operations'. The 'Operations' tab is active. Below the tabs, there is a form for creating a new operation. It includes a required field for 'Name'. Below that is a table with columns 'Label', 'Name', and 'Action'. Under the 'New condition' section, there are two dropdown menus: 'Discovery rule' and 'equals', followed by a text input field 'type here to search' and a 'Select' button. There is an 'Add' link below the dropdowns. An 'Enabled' checkbox is checked. A note states '\* At least one operation must exist.' At the bottom are 'Add' and 'Cancel' buttons. The footer of the page reads 'Zabbix 4.4.1. © 2001–2019, Zabbix SIA'.

4. Complete the **Name** field.
5. Add a new condition.

In the **New condition** section, perform the following actions:

- a. Select **Discovery rule** and **equals** from the drop-down lists.
- b. Click **Select**.
- c. Select the nmap discovery rule.
- d. Click **Add**.

## 2. Configure the operations

1. Click the **Operations** tab.

The screenshot shows the 'Actions' configuration page in Zabbix, specifically the 'Operations' tab. The page has a header 'Actions' and two sub-tabs: 'Action' and 'Operations'. The 'Operations' tab is active. Below the tabs, there is a form for creating a new operation. It includes a 'Default subject' field with the value 'Discovery: (DISCOVERY.DEVICE.STATUS) (DISCOVERY.DEVICE.IPADDRESS)'. Below that is a 'Default message' field with a text area containing several lines of text: 'Discovery rule: (DISCOVERYRULE.NAME)', 'Device IP: (DISCOVERY.DEVICE.IPADDRESS)', 'Device DNS: (DISCOVERY.DEVICE.DNS)', 'Device status: (DISCOVERY.DEVICE.STATUS)', 'Device uptime: (DISCOVERY.DEVICE.uptime)', and 'Device service name: (DISCOVERY.SERVICE.NAME)'. Below the text area is a table with columns 'Details' and 'Action'. There is a 'New' link below the table. A note states '\* At least one operation must exist.' At the bottom are 'Add' and 'Cancel' buttons. The footer of the page reads 'Zabbix 4.4.1. © 2001–2019, Zabbix SIA'.

2. Add the **Add host** operation.
  - a. In the **Operations** section, click **New**.
  - b. In the **Operation details** section, perform the following actions:
    - i. From the **Operation type** drop-down list, select **Add host**.
    - ii. Click **Add**.

The **Add host** operation is added.

The screenshot shows the 'Actions' configuration window in Zabbix. The 'Operations' tab is active. Under 'Default subject', the text is 'Discovery: {DISCOVERY.DEVICE.STATUS} {DISCOVERY.DEVICE.IPADDRESS}'. Under 'Default message', there is a template for a discovery message. In the 'Operations' section, the 'Add host' operation is listed. Below this, a message states '\* At least one operation must exist.' and there are 'Add' and 'Cancel' buttons.

3. Add the **Add to host group** operation.
  - a. In the **Operations** section, click **New**.
  - b. In the **Operation details** section, perform the following actions:
    - i. From the **Operation type** drop-down list, select **Add to host group**.

This screenshot shows the 'Operation details' section of the Zabbix Actions configuration. The 'Operation type' is set to 'Add to host group'. Below this, there is a search field for host groups with the placeholder text 'type here to search' and a 'Select' button. The 'Add' and 'Cancel' buttons are at the bottom. The same '\* At least one operation must exist.' message is present.

- ii. In the **Host groups** field, click **Select**.
- iii. Select **Discovered hosts**.
- iv. Click **Add**.

The **Add to host group** operation is added.

Actions

Default subject: Discovery: {DISCOVERY.DEVICE.STATUS} {DISCOVERY.DEVICE.IPADDRESS}

Default message: Discovery rule: {DISCOVERY.RULE.NAME}

Device IP: {DISCOVERY.DEVICE.IPADDRESS}

Device DNS: {DISCOVERY.DEVICE.DNS}

Device status: {DISCOVERY.DEVICE.STATUS}

Device uptime: {DISCOVERY.DEVICE.UPTIME}

Device service name: {DISCOVERY.SERVICE.NAME}

Operations

Details	Action
<b>Add host</b>	<a href="#">Edit</a> <a href="#">Remove</a>
<b>Add to host groups:</b> Discovered hosts	<a href="#">Edit</a> <a href="#">Remove</a>
<a href="#">New</a>	

\* At least one operation must exist.

[Add](#) [Cancel](#)

Zabbix 4.4.1. © 2001–2019, Zabbix SIA

4. Save the action.

From the main page, click **Add** to complete changes.

The nmap discovery action is created.

✓ Action added

Actions

Event source: Discovery [Create action](#)

Filter

Name:  Status: **Any** Enabled Disabled [Apply](#) [Reset](#)

Name	Conditions	Operations	Status
<input type="checkbox"/> Auto discovery Linux servers	Received value contains Linux Discovery status equals Up Service type equals Zabbix agent Host IP equals XXX.XX.X.1-127,XXX.XX.X.1	<b>Add host</b> <b>Add to host groups:</b> Linux servers <b>Link to templates:</b> Template Hw Atos BullSequanaEdge LLD <b>Enable host</b> <b>Set host inventory mode:</b> Automatic	Disabled
<input type="checkbox"/> mipocket discover	Discovery rule equals mipocket	<b>Add host</b>	Enabled
<input type="checkbox"/> nmap discovery	Discovery rule equals nmap	<b>Add host</b> <b>Add to host groups:</b> Discovered hosts	Enabled

Displaying 3 of 3 found

0 selected [Enable](#) [Disable](#) [Delete](#)

Zabbix 4.4.1. © 2001–2019, Zabbix SIA

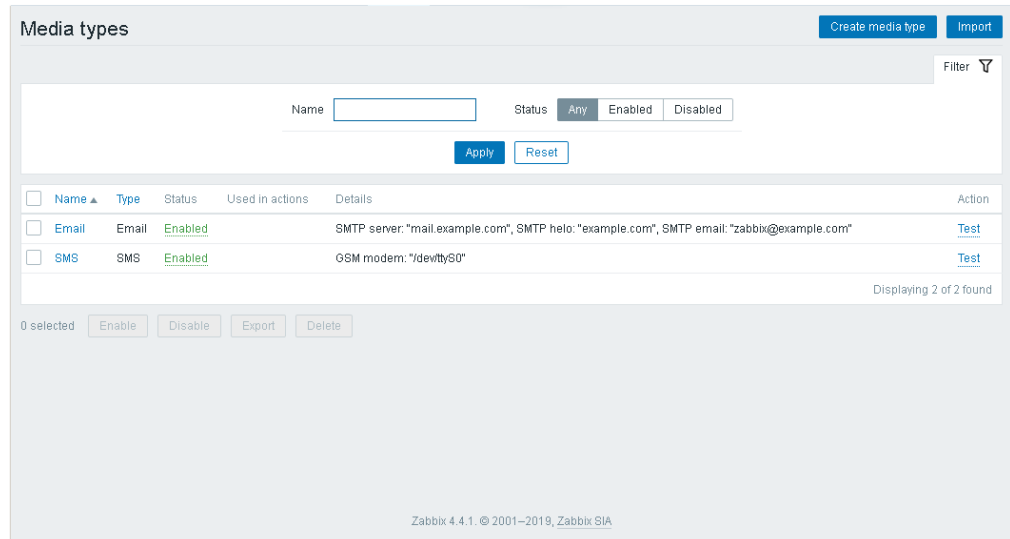
### 3. Check the hosts

From the **Configuration** menu, click **Hosts**.

## 3.9. Setting up email alerts

### 3.9.1. Configuring an mail server

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

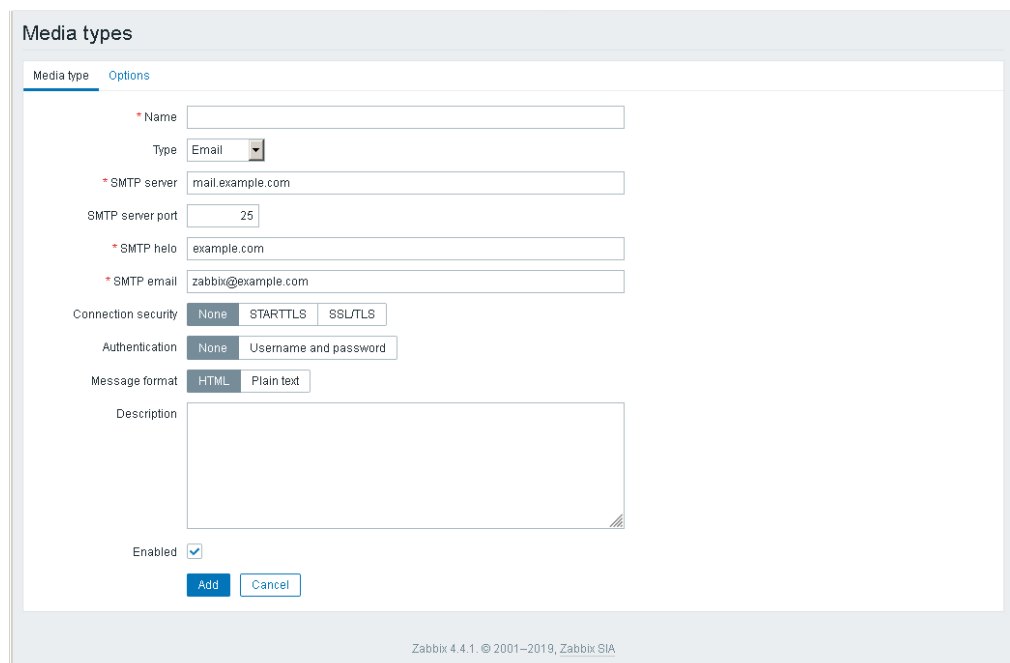


The screenshot shows the 'Media types' page in Zabbix. At the top right are buttons for 'Create media type' and 'Import'. Below them is a search bar with a 'Filter' icon. A table lists the configured media types:

<input type="checkbox"/>	Name	Type	Status	Used in actions	Details	Action
<input type="checkbox"/>	Email	Email	Enabled		SMTP server: "mail.example.com", SMTP helo: "example.com", SMTP email: "zabbix@example.com"	<a href="#">Test</a>
<input type="checkbox"/>	SMS	SMS	Enabled		GSM modem: "devttyS0"	<a href="#">Test</a>

At the bottom, it says 'Displaying 2 of 2 found'. There are also buttons for '0 selected', 'Enable', 'Disable', 'Export', and 'Delete'. The footer indicates 'Zabbix 4.4.1. © 2001–2019, Zabbix SIA'.

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



The screenshot shows the 'Create media type' page. It has tabs for 'Media type' and 'Options'. The 'Media type' tab is active, showing the following fields:

- Name**: A text input field.
- Type**: A dropdown menu with 'Email' selected.
- SMTP server**: A text input field with 'mail.example.com'.
- SMTP server port**: A text input field with '25'.
- SMTP helo**: A text input field with 'example.com'.
- SMTP email**: A text input field with 'zabbix@example.com'.
- Connection security**: Radio buttons for 'None', 'STARTTLS', and 'SSL/TLS'.
- Authentication**: Radio buttons for 'None' and 'Username and password'.
- Message format**: Radio buttons for 'HTML' and 'Plain text'.
- Description**: A large text area.
- Enabled**: A checked checkbox.

At the bottom are 'Add' and 'Cancel' buttons. The footer indicates 'Zabbix 4.4.1. © 2001–2019, Zabbix SIA'.

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.

## Example

The screenshot shows the 'Media types' configuration page in Zabbix. The 'Options' tab is active. The form contains the following fields and options:

- Name:** MyEmail
- Type:** Email (dropdown menu)
- SMTP server:** XXX.XX.X.XX
- SMTP server port:** 25
- SMTP helo:** atos.net
- SMTP email:** XX.XX@atos.net
- Connection security:** None, STARTTLS, SSL/TLS (radio buttons)
- Authentication:** None, Username and password (radio buttons)
- Message format:** HTML, Plain text (radio buttons)
- Description:** (empty text area)
- Enabled:** ☒

At the bottom of the form are 'Add' and 'Cancel' buttons. The footer indicates 'Zabbix 4.4.1. © 2001–2019, Zabbix SIA'.

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

The media type is created.

## Example

The screenshot shows the 'Media types' list page in Zabbix. A green notification banner at the top says 'Media type added'. The page includes a search bar, status filters, and a table of media types.

**Media types list:**

Name	Type	Status	Used in actions	Details	Action
Email	Email	Enabled		SMTP server: "mail.example.com", SMTP helo: "example.com", SMTP email: "zabbix@example.com"	<a href="#">Test</a>
MyEmail	Email	Enabled		SMTP server: "XXX.XX.X.XX", SMTP helo: "atos.net", SMTP email: "XX.XX@atos.net"	<a href="#">Test</a>
SMS	SMS	Enabled		GSM modem: "devttyS0"	<a href="#">Test</a>

At the bottom, there are buttons for '0 selected', 'Enable', 'Disable', 'Export', and 'Delete'. The footer indicates 'Zabbix 4.4.1. © 2001–2019, Zabbix SIA'.

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

### 3.9.2. Creating an action

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

Actions

Event source: Triggers [Create action](#)

Name  Status: [Any](#) [Enabled](#) [Disabled](#)

[Apply](#) [Reset](#)

<input type="checkbox"/>	Name	Conditions	Operations	Status
<input type="checkbox"/>	Report problems to Zabbix administrators		Send message to user groups: Zabbix administrators via all media	Disabled

0 selected [Enable](#) [Disable](#) [Delete](#)

Displaying 1 of 1 found

Zabbix 4.4.1. © 2001–2019, Zabbix SIA

2. From the **Event source** drop-down list, select **Triggers**.
3. Click the **Create action** button. A new page opens.

Actions

[Action](#) [Operations](#) [Recovery operations](#) [Update operations](#)

\* Name

Conditions

Label	Name	Action
-------	------	--------

New condition

Trigger name  contains

[Add](#)

Enabled ☒

\* At least one operation, recovery operation or update operation must exist.

[Add](#) [Cancel](#)

<https://172.31.131.101:4443/zabbix.php?action=dashboard.view>

Zabbix 4.4.1. © 2001–2019, Zabbix SIA

4. Complete the **Name** field.

5. Click the **Operations** tab.

Actions

Action Operations Recovery operations Update operations

\* Default operation step duration 1h

Default subject Problem: {EVENT.NAME}

Default message Problem started at {EVENT.TIME} on {EVENT.DATE}  
Problem name: {EVENT.NAME}  
Host: {HOST.NAME}  
Severity: {EVENT.SEVERITY}  
Original problem ID: {EVENT.ID}  
{TRIGGER.URL}

Pause operations for suppressed problems ☒

Operations Steps Details Start in Duration Action

[New](#)

\* At least one operation, recovery operation or update operation must exist.

[Add](#) [Cancel](#)

Zabbix 4.4.1. © 2001–2019, Zabbix SIA

6. In the **Operations** section, click **New**.

Actions

Action Operations Recovery operations Update operations

\* Default operation step duration 1h

Default subject Problem: {EVENT.NAME}

Default message Problem started at {EVENT.TIME} on {EVENT.DATE}  
Problem name: {EVENT.NAME}  
Host: {HOST.NAME}  
Severity: {EVENT.SEVERITY}  
Original problem ID: {EVENT.ID}  
{TRIGGER.URL}

Pause operations for suppressed problems ☒

Operations Steps Details Start in Duration Action

Operation details

Steps 1 - 1 (0 - infinitely)

Step duration 0 (0 - use action default)

Operation type Send message

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

Send to User groups User group Action

[Add](#)

Send to Users User Action

[Add](#)

Send only to - All -

Default message ☒

Conditions Label Name Action

[New](#)

[Add](#) [Cancel](#)

\* At least one operation, recovery operation or update operation must exist.

[Add](#) [Cancel](#)

Zabbix 4.4.1. © 2001–2019, Zabbix SIA



7. In the **Operation details** section, perform the following actions:
  - a. Add the message recipient
 

If the recipient is a user:

    - i. In the **Send to Users** section, click **Add**.
    - ii. Select the user required.

If the recipient is a user group:

    - i. In the **Send to User groups** section, click **Add**.
    - ii. Select the user group required.
  - b. From the **Send only to** drop-down list, select the media type previously created.
  - c. Click **Add**.

### Example

The screenshot shows the 'Actions' configuration page in Zabbix, specifically the 'Operations' tab. At the top, there are tabs for 'Action', 'Operations', 'Recovery operations', and 'Update operations'. The 'Default operation step duration' is set to '1h'. The 'Default subject' is 'Problem: {EVENT.NAME}'. The 'Default message' contains a template: 'Problem started at {EVENT.TIME} on {EVENT.DATE}. Problem name: {EVENT.NAME}. Host: {HOST.NAME}. Severity: {EVENT.SEVERITY}. Original problem ID: {EVENT.ID} ({TRIGGER.URL})'. There is a checkbox for 'Pause operations for suppressed problems' which is checked. Below this is a table with columns 'Operations', 'Steps', 'Details', 'Start in', 'Duration', and 'Action'. It contains one entry: '1 Send message to users: Admin (Zabbix Administrator) via MyEmail Immediately Default' with links for 'Edit' and 'Remove'. At the bottom, there is a note: '\* At least one operation, recovery operation or update operation must exist.' and buttons for 'Add' and 'Cancel'.

8. Save the action.
- Click **Add** to complete changes.
- The action is created.

### Example

The screenshot shows the 'Actions' list page in Zabbix. At the top, there is a green notification bar that says 'Action added'. Below it, there is a search bar and a 'Filter' button. The main table has columns for 'Name', 'Conditions', 'Operations', and 'Status'. It lists two actions: 'Report problems to Zabbix administrators' (Status: Disabled) and 'Send message to users: Admin (Zabbix Administrator) via MyEmail' (Status: Enabled). At the bottom, there are buttons for 'Enable', 'Disable', and 'Delete'.

### 3.9.3. Configuring the user

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

Users

User group: All [Create user](#)

Filter

Alias  Name  Surname  User type: Any Zabbix User Zabbix Admin Zabbix Super Admin

[Apply](#) [Reset](#)

<input type="checkbox"/>	Alias	Name	Surname	User type	Groups	Is online?	Login	Frontend access	Debug mode	Status
<input type="checkbox"/>	Admin	Zabbix	Administrator	Zabbix Super Admin	Zabbix administrators	Yes (2020-02-26 14:02:54)	Ok	System default	Disabled	Enabled
<input type="checkbox"/>	guest			Zabbix User	Guests	No (2020-02-26 13:21:27)	Ok	Internal	Disabled	Enabled

0 selected [Unlock](#) [Delete](#)

Displaying 2 of 2 found

Zabbix 4.4.1. © 2001–2019, Zabbix SIA

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

Users

User Media Permissions

Media

Media	Type	Send to	When active	Use if severity	Status	Action
<a href="#">Add</a>						

[Update](#) [Delete](#) [Cancel](#)

Zabbix 4.4.1. © 2001–2019, Zabbix SIA

4. In the **Media** section, click **Add**. The **Media** page opens.

### Example

The screenshot shows the Zabbix Users page with the 'Media' tab selected. A modal window titled 'Media' is open, allowing configuration of a new media type. The 'Type' dropdown is set to 'MyEmail'. The 'Send to' field is empty, with a 'Remove' link next to it. The 'When active' field is set to '1-7,00:00-24:00'. Under 'Use if severity', the checkboxes for 'Not classified', 'Information', and 'Warning' are unchecked, while 'Average', 'High', and 'Disaster' are checked. The 'Enabled' checkbox is also checked. 'Add' and 'Cancel' buttons are at the bottom right of the modal.

- a. From the **Type** drop-down list, select the media type previously created.
- b. Complete the fields as required.
- c. Click **Add**.

### Example

The screenshot shows the Zabbix Users page with the 'Media' tab selected. A table displays the configured media types. The table has columns for 'Media', 'Type', 'Send to', 'When active', 'Use if severity', 'Status', and 'Action'. One media type is listed: 'MyEmail' with 'Send to' 'XX.XX@yatos.net', 'When active' '1-7,00:00-24:00', 'Use if severity' 'High', and 'Status' 'Enabled'. Below the table are 'Add', 'Update', 'Delete', and 'Cancel' buttons.

Media	Type	Send to	When active	Use if severity	Status	Action
MyEmail	XX.XX@yatos.net	1-7,00:00-24:00	High	Enabled	Edit Remove	

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

## 3.10. Setting up SMS alerts

This procedure uses the zabbix-smsmode script. It allows a SMS to be sent via the smsmode provider.

---

**Note** The zabbix-smsmode script is delivered in a sub-directory of the MISM installation directory: `\zabbix\server>alertscripts`.

---

### Prerequisites

Zabbix-smsmode script is available.

<https://www.smsmode.com/en/> is accessible by the server.

An access key has been created.

---

**See** The smsmode site to generate an access key:  
<https://ui.smsmode.com/>.

---

### 3.10.1. Configuring the SMS

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

The screenshot shows the 'Media types' configuration page in the Zabbix Management Console. At the top right, there are buttons for 'Create media type' and 'Import'. Below these is a search bar with a 'Filter' icon. The main content area contains a table with columns: Name, Type, Status, Used in actions, Details, and Action. There are two entries: 'Email' and 'SMS', both with a status of 'Enabled'. Below the table, there are buttons for 'Apply' and 'Reset'. At the bottom, there are buttons for 'Enable', 'Disable', 'Export', and 'Delete'. The footer indicates 'Zabbix 4.4.1. © 2001–2019, Zabbix SIA'.

Name	Type	Status	Used in actions	Details	Action
Email	Email	Enabled		SMTP server: "mail.example.com", SMTP helo: "example.com", SMTP email: "zabbix@example.com"	Test
SMS	SMS	Enabled		GSM modem: "/dev/ttyS0"	Test

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

Media types

Media type Options

\* Name

Type

\* SMTP server

SMTP server port

\* SMTP helo

\* SMTP email

Connection security

Authentication

Message format

Description

Enabled ☒

Zabbix 4.4.1. © 2001–2019, Zabbix SIA

3. Complete the **Name** field.
4. Select **Script** from the **Type** drop-down list.
5. Enter **zabbix-smsmode** in the **Script name** field.
6. In the **Script parameters** section, add the following settings.

Parameter	Value
--message	{ALERT.SUBJECT} - {ALERT.MESSAGE}
--to	{ALERT.SENDTO}
--accessToken	Acces key generated by smsmode

Example

Media types

Media type

Options

Name

SMS France

Type

Script

Script name

zabbix-smsmode

Script parameters

Parameter

Action

--message={ALERT.SUBJECT} - {ALERT.MESSAGE}

Remove

--to={ALERT.SENDTO}

Remove

--accessTokenIdRIBx/SW/m5G8wekCkhlYDaf2aMPol

Remove

Add

Description

Enabled

☒

Add

Cancel

7. Click **Add** to complete changes.
- The media type is created.

Example

Media types

Create media typeImport

Filter

Name

Status

AnyEnabledDisabled

ApplyReset

<input type="checkbox"/>	Name	Type	Status	Used in actions	Details	Action
<input type="checkbox"/>	Email	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
<input type="checkbox"/>	SMS France	Script	Enabled		Script name: "zabbix-smsmode"	Test

0 selectedEnableDisableExportDelete

Displaying 3 of 3 found

Zabbix 4.4.1. © 2001–2019, Zabbix SIA

8. Click **Test** to send a test SMS.

### 3.10.2. Creating an action

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

Actions

Event source: Triggers [Create action](#)

Name  Status: [Any](#) [Enabled](#) [Disabled](#)

[Apply](#) [Reset](#)

<input type="checkbox"/>	Name	Conditions	Operations	Status
<input type="checkbox"/>	Report problems to Zabbix administrators		Send message to user groups: Zabbix administrators via all media	Disabled

0 selected [Enable](#) [Disable](#) [Delete](#)

Displaying 1 of 1 found

Zabbix 4.4.1. © 2001–2019, Zabbix SIA

2. From the **Event source** drop-down list, select **Triggers**.
3. Click the **Create action** button. A new page opens.

Actions

[Action](#) [Operations](#) [Recovery operations](#) [Update operations](#)

\* Name

Conditions Label Name Action

New condition

Trigger name  contains

[Add](#)

Enabled ☒

\* At least one operation, recovery operation or update operation must exist.

[Add](#) [Cancel](#)

<https://172.31.131.101:4443/zabbix.php?action=dashboard.view>

Zabbix 4.4.1. © 2001–2019, Zabbix SIA

4. Complete the **Name** field.

5. Click the **Operations** tab.

**Actions**

[Action](#) [Operations](#) [Recovery operations](#) [Update operations](#)

\* Default operation step duration:

Default subject:

Default message:   
Problem name: {EVENT.NAME}  
Host: {HOST.NAME}  
Severity: {EVENT.SEVERITY}  
  
Original problem ID: {EVENT.ID}  
{TRIGGER.URL}"/>

Pause operations for suppressed problems: ☒

Operations: [Steps](#) [Details](#) [Start in](#) [Duration](#) [Action](#)

\* At least one operation, recovery operation or update operation must exist.

[Add](#) [Cancel](#)

Zabbix 4.4.1. © 2001–2019, Zabbix SIA

6. In the **Operations** section, click **New**.

**Actions**

[Action](#) [Operations](#) [Recovery operations](#) [Update operations](#)

\* Default operation step duration:

Default subject:

Default message:   
Problem name: {EVENT.NAME}  
Host: {HOST.NAME}  
Severity: {EVENT.SEVERITY}  
  
Original problem ID: {EVENT.ID}  
{TRIGGER.URL}"/>

Pause operations for suppressed problems: ☒

Operations: [Steps](#) [Details](#) [Start in](#) [Duration](#) [Action](#)

Operation details

Steps:  -  (0 - infinitely)

Step duration:  (0 - use action default)

Operation type:

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

Send to User groups:  [Add](#) [Action](#)

Send to Users:  [Add](#) [Action](#)

Send only to:

Default message: ☒

Conditions: 

Label	Name	Action
		<a href="#">New</a>

[Add](#) [Cancel](#)

\* At least one operation, recovery operation or update operation must exist.

[Add](#) [Cancel](#)

Zabbix 4.4.1. © 2001–2019, Zabbix SIA



7. In the **Operation details** section, perform the following actions:
  - a. Add the message recipient

If the recipient is a user:

  - i. In the **Send to Users** section, click **Add**.
  - ii. Select the user required.

If the recipient is a user group:

  - i. In the **Send to User groups** section, click **Add**.
  - ii. Select the user group required.
  - b. From the **Send only to** drop-down list, select the media type previously created.
  - c. Click **Add**.

### Example

The screenshot shows the Zabbix 'Actions' configuration window, specifically the 'Operations' tab. At the top, there are tabs for 'Action', 'Operations', 'Recovery operations', and 'Update operations'. Below these, there are fields for 'Default operation step duration' (set to 1h), 'Default subject' (set to 'Problem: {EVENT.NAME}'), and 'Default message' (containing a template with variables like {EVENT.TIME}, {EVENT.DATE}, {EVENT.NAME}, {HOST.NAME}, {EVENT.SEVERITY}, and {EVENT.ID}). There is a checkbox for 'Pause operations for suppressed problems' which is checked. Below this is a table with columns 'Steps', 'Details', 'Start in', 'Duration', and 'Action'. The table contains one row with '1' in the 'Steps' column and 'Send message to users: Admin (Zabbix Administrator) via SMS France' in the 'Details' column. The 'Duration' is 'Immediately' and the 'Action' is 'Default'. There are 'Edit' and 'Remove' links for this operation. At the bottom, there is a message: '\* At least one operation, recovery operation or update operation must exist.' and 'Add' and 'Cancel' buttons.

8. Save the action.
- Click **Add** to complete changes.
- The action is created.

## Example

The screenshot shows the Zabbix Actions configuration interface. At the top, there's a header with a green checkmark and the text "Action added". Below this, the "Actions" tab is selected. On the right, there's a dropdown for "Event source" set to "Triggers" and a "Create action" button. A filter icon is also present. Below the header, there's a search bar for "Name" and a status filter with options "Any", "Enabled", and "Disabled". There are "Apply" and "Reset" buttons. The main table lists two actions:

<input type="checkbox"/>	Name	Conditions	Operations	Status
<input type="checkbox"/>	Report problems to Zabbix administrators		Send message to user groups: Zabbix administrators via all media	Disabled
<input type="checkbox"/>	testPB		Send message to users: Admin (Zabbix Administrator) via SMS France	Enabled

At the bottom, it says "0 selected" and has buttons for "Enable", "Disable", and "Delete". The footer indicates "Zabbix 4.4.1. © 2001–2019, Zabbix SIA".

### 3.10.3. Configuring the user

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

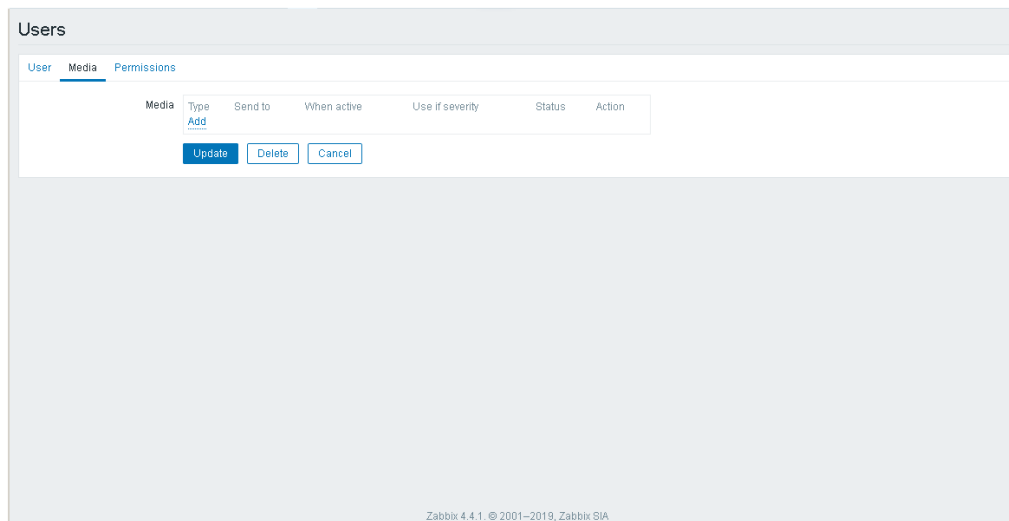
The screenshot shows the Zabbix Users configuration interface. At the top, there's a header with the text "Users". On the right, there's a dropdown for "User group" set to "All" and a "Create user" button. A filter icon is also present. Below the header, there's a search bar for "Alias", "Name", and "Surname". There's also a "User type" filter with options "Any", "Zabbix User", "Zabbix Admin", and "Zabbix Super Admin". There are "Apply" and "Reset" buttons. The main table lists two users:

<input type="checkbox"/>	Alias	Name	Surname	User type	Groups	Is online?	Login	Frontend access	Debug mode	Status
<input type="checkbox"/>	Admin	Zabbix	Administrator	Zabbix Super Admin	Zabbix administrators	Yes (2020-02-26 14:02:54)	Ok	System default	Disabled	Enabled
<input type="checkbox"/>	guest			Zabbix User	Guests	No (2020-02-26 13:21:27)	Ok	Internal	Disabled	Enabled

At the bottom, it says "0 selected" and has buttons for "Unblock" and "Delete". The footer indicates "Zabbix 4.4.1. © 2001–2019, Zabbix SIA".

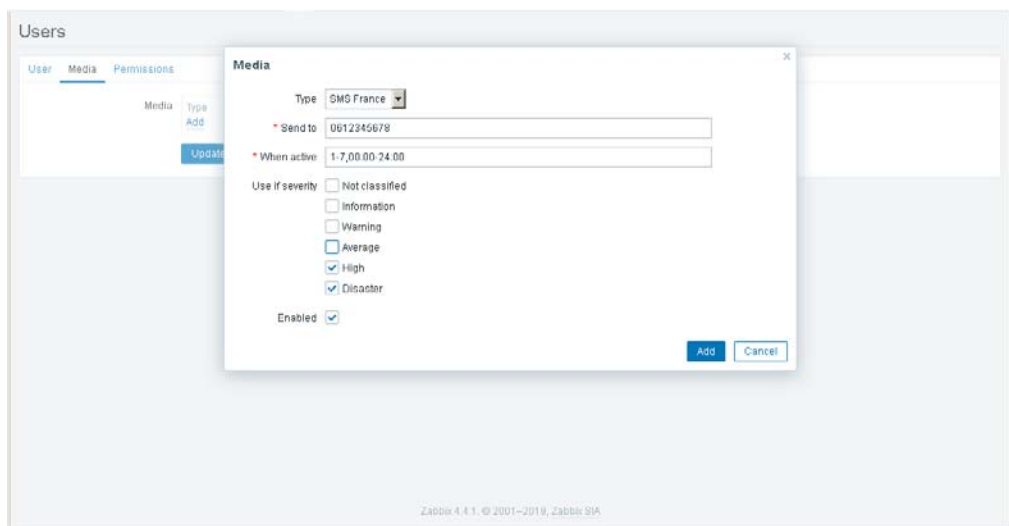
2. Select the user required. A new page opens.

3. Click the **Media** tab.



4. In the **Media** section, click **Add**. The **Media** page opens.

### Example



- From the **Type** drop-down list, select the media type previously created.
- Complete the fields as required.
- Click **Add**.

## Example

The screenshot shows the 'Users' management interface in Zabbix. The 'Media' tab is selected, displaying a table of media entries for a user. The table has columns for Type, Send to, When active, Use if severity, Status, and Action. A single entry is shown: 'SMS France' with '0812345678' as the contact, active from '1-7,00:00-24:00', and associated with 'Warning' severity. The status is 'Enabled'. Below the table are buttons for 'Add', 'Update', 'Delete', and 'Cancel'. The footer indicates 'Zabbix 4.4.1. © 2001-2019, Zabbix SIA'.

Type	Send to	When active	Use if severity	Status	Action
SMS France	0812345678	1-7,00:00-24:00	Warning	Enabled	Edit Remove

[Add](#) [Update](#) [Delete](#) [Cancel](#)

Zabbix 4.4.1. © 2001-2019, Zabbix SIA

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

## 3.11. Monitoring resources

---

**See** Zabbix documentation for more information:  
[https://www.zabbix.com/documentation/4.4/manual/web\\_interface/frontend\\_sections/monitoring](https://www.zabbix.com/documentation/4.4/manual/web_interface/frontend_sections/monitoring)

---

Click the **Monitoring** menu to display the information.

### 3.11.1. Dashboard

Click the **Dashboard** tab to display summaries of all the important information.

A dashboard consists of widgets and each widget is designed to display information of a certain kind and source, which can be a summary, a map, a graph, the clock, etc.

Widgets are added and edited in the dashboard editing mode. Widgets are viewed in the dashboard viewing mode.

While in a single dashboard you can group widgets from various sources for a quick overview, it is also possible to create several dashboards containing different sets of overviews and switch between them.

The time period that is displayed in graph widgets is controlled by the time period section located above the widgets. The time period selector label, located to the right, displays the currently selected time period. Clicking the tab label expands and collapses the time period selector.

Note that when the dashboard is displayed in kiosk mode (accessible from the full screen mode) and widgets only are displayed, it is possible to zoom out the graph period by double clicking in the graph.

#### Host menu

Click a host in the **Problems** widget to bring up the host menu. It includes links to inventory, latest data, problems, graphs and screens for the host.

### 3.11.2. Problems

Click the **Problems** tab to display current problems. Problems are triggers that are in the Problem state.

#### Host menu

Click a host in the **Problems** section to bring up the host menu. It includes links to inventory, latest data, problems, graphs and screens for the host.

### 3.11.3. Overview

Click the **Overview** tab to display an overview of trigger states or a comparison of data for various hosts at once.

#### Host menu

Click a host in the **Overview** section (**Hosts: left**) to bring up the host menu. It includes links to inventory, latest data, problems, graphs and screens for the host.

### 3.11.4. Web

Click the **Web** tab to display current information about web scenarios.

### 3.11.5. Latest data

Click the **Latest data** tab to view the latest values gathered by items as well as to access various graphs for the items.

#### Host menu

Click a host in the **Latest data** section to bring up the host menu. It includes links to inventory, latest data, problems, graphs and screens for the host.

### 3.11.6. Graphs

Click the **Graphs** tab to display any custom graph that has been configured.

### 3.11.7. Screens

Click the **Screens** tab to configure, manage and view Zabbix global screens and slide shows.

#### Host menu

Click a host in the **Screens** section (in **Host issues** and **Host group issues** widgets) to bring up the host menu. It includes links to inventory, latest data, problems, graphs and screens for the host.

### 3.11.8. Maps

Click the **Maps** tab to configure, manage and view network maps.

#### Host menu

Click a host in the **Maps** section to bring up the host menu. It includes links to inventory, latest data, problems, graphs and screens for the host.

### 3.11.9. Discovery

Click the **Discovery** tab to review results of network discovery. Discovered devices are sorted by the discovery rule.

### 3.11.10. Services

Click the **Services** to review the status of IT infrastructure or business services.



**Bull Cedoc  
357 avenue Patton  
BP 20845  
49008 Angers Cedex 01  
FRANCE**