

# 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 2021

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**

**October 2021**

**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
1.2.1. Installing the MISM console .....	1-2
1.2.2. Updating the MISM console .....	1-4
1.3. Controlling the MISM console .....	1-6
1.4. Changing the connection certificate .....	1-7
1.5. Configuring a proxy server .....	1-8
1.6. Recovering MISM databases .....	1-9
<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 .....	2-9
2.4. Controlling resources .....	2-11
2.4.1. Available job templates .....	2-11
2.4.2. Launching a job .....	2-14
2.4.3. Scheduling a job .....	2-17
2.5. Adding security .....	2-20
2.5.1. Creating a password for the BullSequana Edge Vault .....	2-20
2.5.2. Creating an encrypted password for a host .....	2-22
2.5.3. Deleting an encrypted password .....	2-23
2.6. Setting up email alerts .....	2-24
2.6.1. Creating an email notification template .....	2-24
2.6.2. Assigning a notification to a job template .....	2-26
2.7. Performing basic operations .....	2-27
2.7.1. Performing power operations .....	2-27
2.7.2. Updating firmware .....	2-29
2.7.3. Enabling syslog forwarding .....	2-32

<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	3-4
3.3. Preliminary configuration	3-5
3.3.1. Enabling automatic inventory	3-5
3.3.2. Renaming the Zabbix server host	3-6
3.4. Managing the 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	3-19
3.6.3. Creating an encrypted password for a host	3-21
3.7. Enabling syslog forwarding	3-23
3.7.1. Importing the Atos Rsyslog template	3-23
3.7.2. Linking the Zabbix server host to the Atos Rsyslog template	3-25
3.7.3. Displaying the logs	3-26
3.8. Configuring nmap	3-27
3.8.1. Creating a nmap discovery rule	3-27
3.8.2. Creating a nmap action	3-29
3.9. Setting up email alerts	3-33
3.9.1. Configuring an mail server	3-33
3.9.2. Creating an action	3-35
3.9.3. Configuring the user	3-38
3.10. Setting up SMS alerts	3-40
3.10.1. Configuring the SMS	3-40
3.10.2. Creating an action	3-43
3.10.3. Configuring the user	3-46
3.11. Monitoring resources	3-48
3.11.1. Dashboard	3-48
3.11.2. Problems	3-48
3.11.3. Overview	3-48
3.11.4. Web	3-49
3.11.5. Latest data	3-49
3.11.6. Graphs	3-49
3.11.7. Screens	3-49
3.11.8. Maps	3-49
3.11.9. Discovery	3-49
3.11.10. Services	3-49

---

## 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.

There are two separate deliverables for MISM:

- MISM\_full\_<version>.tar.gz for full installation
- MISM\_light\_<version>.tar.gz for update, which contains only AWX playbooks, AWX plugins, Zabbix templates, Zabbix external scripts and shell scripts

---

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

---

### 1.2.1. Installing the MISM console

#### 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\_full\_<version>.tar.gz package is available

#### Estimated operation time

15 minutes

#### Procedure

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

```
$ tar xzvf mism_full_<version>.tar.gz
```

4. Launch the installation.

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

---

**Notes** • Performed on an existing installation, this operation preserves user data such as inventories and user accounts

- Ansible installation is optional

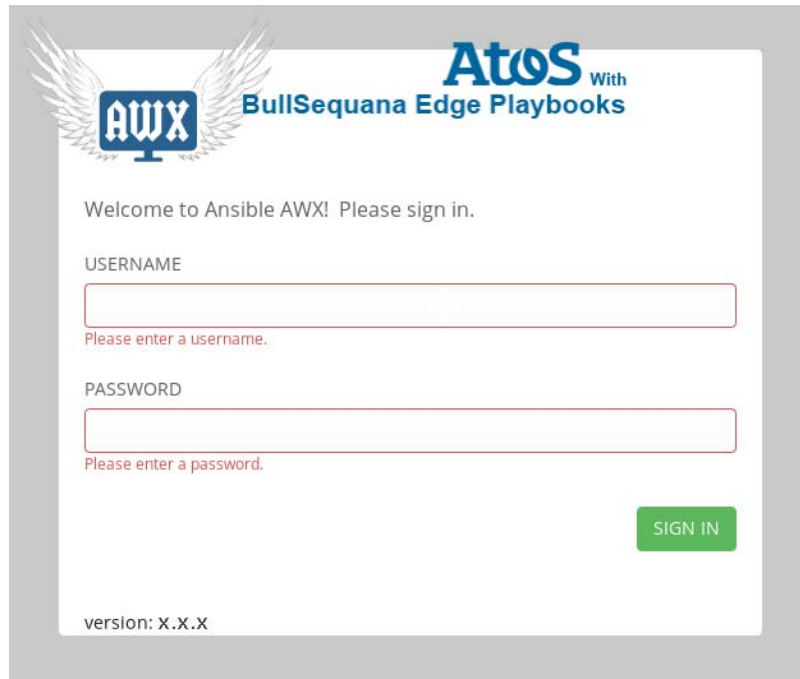
5. When the request to confirm the installation of Ansible appears, answer Yes or No as required.

6. Start the MISM console.

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



7. Open a web browser.
8. Connect to the MISM console by entering the name or IP address of the MISM console in the address bar, using the https protocol.
9. Wait until the update is complete and the authentication page opens.



10. Add the playbooks.

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

```
$. /add_ansible_playbooks_and_plugins.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.

---

## 1.2.2. Updating the MISM console

### 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\_light\_<version>.tar.gz package is available

### Estimated operation time

15 minutes

### Procedure

1. Open a terminal window.
2. Go to the installation directory.
3. Stop the MISM console.

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

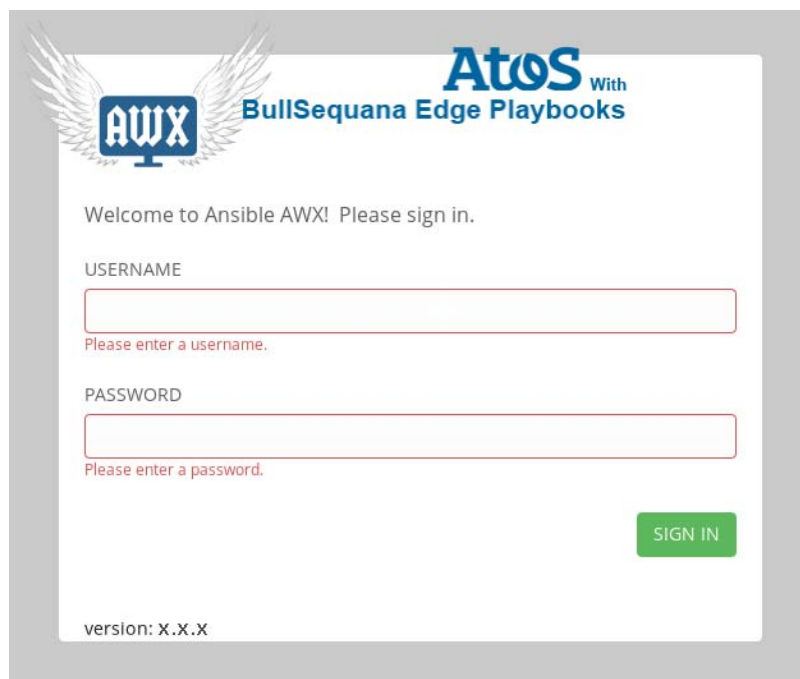
4. Extract the MISM file.

```
$ tar xzvf mism_light.<version>.tar.gz
```

5. Start the MISM console.

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

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.



## 9. Add the playbooks.

```
$. /add_aws_playbooks.sh
```

```
$. /add_aws_playbooks_and_plugins.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
```

## 1.6. Recovering MISM databases

This section explains how to backup and restore the AWX and Zabbix databases.

- 
- Notes**
- The commands are located in the MISM installation directory
  - The backup files are located in the `installation_directory/storage/pgadmin_bullsequana.com/` directory
- 

### Recovering an AWX database

- To backup the AWX database, run the following command:

```
./backup_database.sh -t awx -f backup_file
```

- To restore the AWX database, run the following command:

```
./restore_database.sh -t awx -f backup_file
```

### Recovering a Zabbix database

- To backup the Zabbix database, run the following command:

```
./backup_database.sh -t zabbix -f backup_file
```

- To restore the Zabbix database, run the following command:

```
./restore_database.sh -t zabbix -f backup_file
```





---

## 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.

---

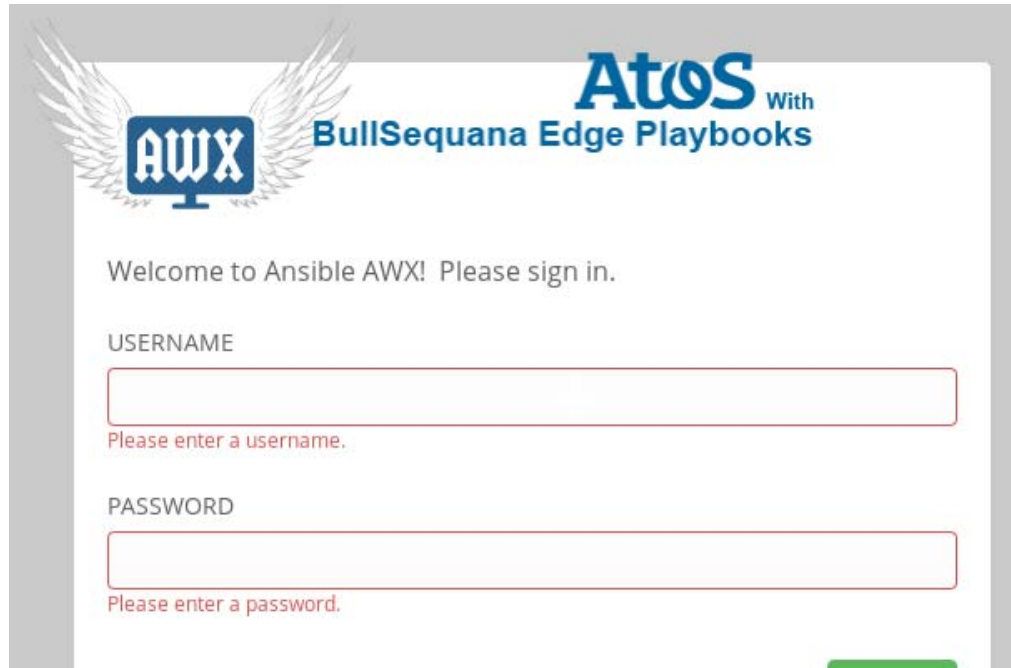
**Important** Consult the full Ansible Tower documentation before using the MISM console:  
<https://docs.ansible.com/ansible-tower/>

---

## 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

The screenshot shows the Atos console dashboard. On the left is a dark sidebar menu with sections: VIEWS (Dashboard, Jobs, Schedules, My View), RESOURCES (Templates, Credentials, Projects, Inventories, Inventory Scripts), ACCESS (Organizations, Users, Teams), and ADMINISTRATION (Credential Types, Notifications, Management Jobs, Instance Groups, Applications, Settings). The main area is titled 'DASHBOARD' and contains several widgets. At the top right, a user profile 'mijm' and several icons are visible, labeled 'E'. Below this is a summary row with six cards: 1 HOSTS, 1 FAILED HOSTS, 1 INVENTORIES, 0 INVENTORY SYNC FAILURES, 1 PROJECTS, and 0 PROJECT SYNC FAILURES. A 'JOB STATUS' line chart shows job counts over time from May 19 to Jun 19. Below the chart are two tables: 'RECENTLY USED TEMPLATES' and 'RECENT JOB RUNS'. Annotations A through D point to the corresponding menu sections in the sidebar.

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:

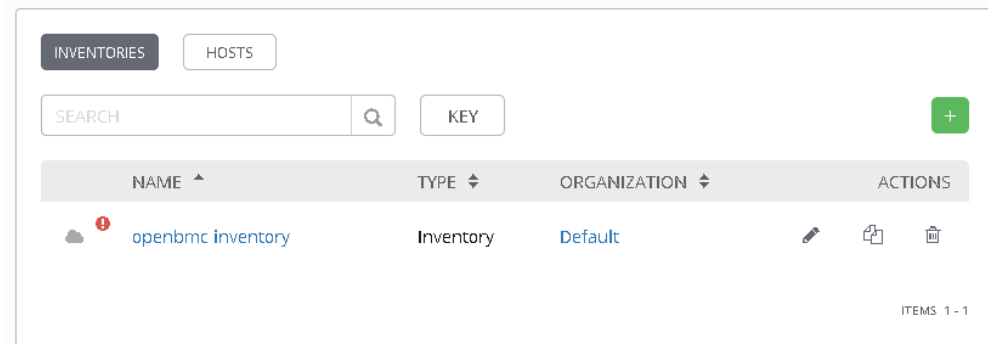
- The BullSequana Edge Playbooks project, which contains the delivered playbooks
- A collection of job templates, which are based on the provided playbooks
- The BullSequana Edge inventory, given as an example
- The Bull organization
- The BullSequana Edge group
- The BullSequana Edge Vault credential

## 2.3. Adding resources

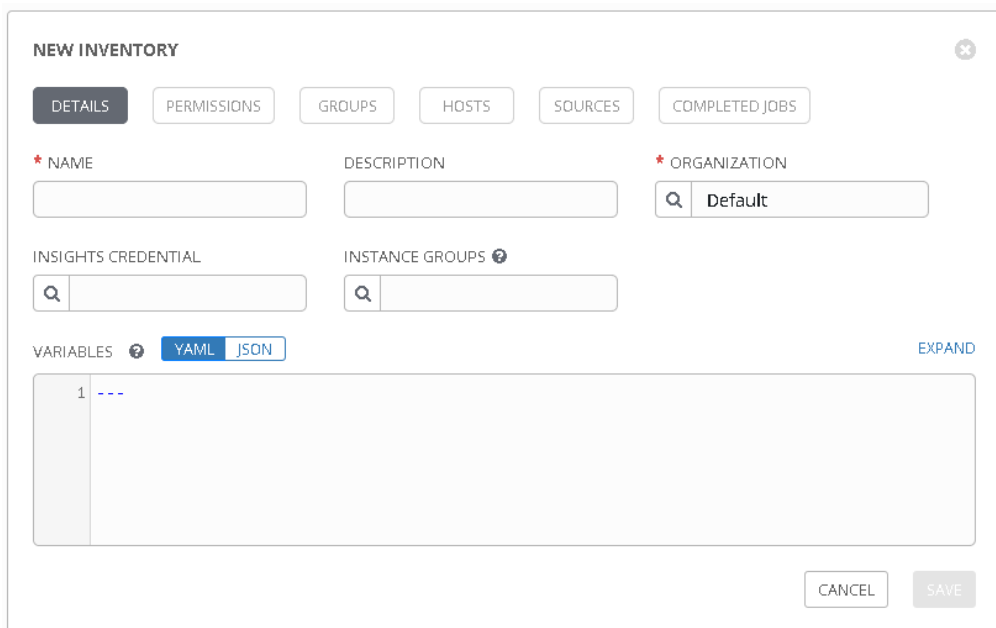
### 2.3.1. Creating an inventory

**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.

A screenshot of the 'NEW INVENTORY' form in the OpenBMC web interface. The form has a title 'NEW INVENTORY' and a close button. Below the title are several tabs: 'DETAILS', 'PERMISSIONS', 'GROUPS', 'HOSTS', 'SOURCES', and 'COMPLETED JOBS'. The 'DETAILS' tab is selected. The form contains several input fields: '\* NAME' (required), 'DESCRIPTION', '\* ORGANIZATION' (required), 'INSIGHTS CREDENTIAL', and 'INSTANCE GROUPS'. There are also search icons next to the 'INSIGHTS CREDENTIAL' and 'INSTANCE GROUPS' fields. Below these fields is a 'VARIABLES' section with a dropdown menu set to 'YAML' and 'JSON' buttons. The 'VARIABLES' section shows a list with one item '1 ---'. At the bottom right of the form 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.

5. 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.

---

6. Click **Save**.



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

1. 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 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 **Groups**.
3. Click the green + button. The **Create Group** page opens.

CREATE GROUP

DETAILS GROUPS HOSTS

\* NAME DESCRIPTION

VARIABLES **YAML** JSON

```
1 ---
```

CANCEL SAVE

4. Complete the required fields and click **Save**.
5. Click **Hosts**.

6. Click the green + button and select **Existing Host**. The **Select Hosts** window opens.

**SELECT HOSTS** ✕

SEARCH Q KEY

HOSTS ▲

ON XXX.XX.XX.XX

ITEMS 1 - 1

CANCEL SAVE

7. 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	
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>

<b>Name</b>	<b>Description</b>	<b>Necessary variables</b>
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

		Compact	Expanded
<a href="#">activate firmware update</a>	Job Template	<div style="display: flex; gap: 2px;"><div style="width: 10px; height: 10px; background-color: #28a745;"></div><div style="width: 10px; height: 10px; background-color: #ccc;"></div><div style="width: 10px; height: 10px; background-color: #ccc;"></div><div style="width: 10px; height: 10px; background-color: #ccc;"></div><div style="width: 10px; height: 10px; background-color: #ccc;"></div><div style="width: 10px; height: 10px; background-color: #ccc;"></div><div style="width: 10px; height: 10px; background-color: #ccc;"></div><div style="width: 10px; height: 10px; background-color: #ccc;"></div><div style="width: 10px; height: 10px; background-color: #ccc;"></div><div style="width: 10px; height: 10px; background-color: #ccc;"></div><div style="width: 10px; height: 10px; background-color: #ccc;"></div><div style="width: 10px; height: 10px; background-color: #ccc;"></div><div style="width: 10px; height: 10px; background-color: #ccc;"></div><div style="width: 10px; height: 10px; background-color: #ccc;"></div><div style="width: 10px; height: 10px; background-color: #ccc;"></div><div style="width: 10px; height: 10px; background-color: #ccc;"></div><div style="width: 10px; height: 10px; background-color: #ccc;"></div><div style="width: 10px; height: 10px; background-color: #ccc;"></div><div style="width: 10px; height: 10px; background-color: #ccc;"></div></div>	  
<a href="#">check critical alarms</a>	Job Template	<div style="display: flex; gap: 2px;"><div style="width: 10px; height: 10px; background-color: #28a745;"></div><div style="width: 10px; height: 10px; background-color: #ccc;"></div><div style="width: 10px; height: 10px; background-color: #ccc;"></div><div style="width: 10px; height: 10px; background-color: #ccc;"></div><div style="width: 10px; height: 10px; background-color: #ccc;"></div><div style="width: 10px; height: 10px; background-color: #ccc;"></div><div style="width: 10px; height: 10px; background-color: #ccc;"></div><div style="width: 10px; height: 10px; background-color: #ccc;"></div><div style="width: 10px; height: 10px; background-color: #ccc;"></div><div style="width: 10px; height: 10px; background-color: #ccc;"></div><div style="width: 10px; height: 10px; background-color: #ccc;"></div><div style="width: 10px; height: 10px; background-color: #ccc;"></div><div style="width: 10px; height: 10px; background-color: #ccc;"></div><div style="width: 10px; height: 10px; background-color: #ccc;"></div><div style="width: 10px; height: 10px; background-color: #ccc;"></div><div style="width: 10px; height: 10px; background-color: #ccc;"></div><div style="width: 10px; height: 10px; background-color: #ccc;"></div><div style="width: 10px; height: 10px; background-color: #ccc;"></div><div style="width: 10px; height: 10px; background-color: #ccc;"></div></div>	  
<a href="#">check power off</a>	Job Template	<div style="display: flex; gap: 2px;"><div style="width: 10px; height: 10px; background-color: #dc3545;"></div><div style="width: 10px; height: 10px; background-color: #28a745;"></div><div style="width: 10px; height: 10px; background-color: #ccc;"></div><div style="width: 10px; height: 10px; background-color: #ccc;"></div><div style="width: 10px; height: 10px; background-color: #ccc;"></div><div style="width: 10px; height: 10px; background-color: #ccc;"></div><div style="width: 10px; height: 10px; background-color: #ccc;"></div><div style="width: 10px; height: 10px; background-color: #ccc;"></div><div style="width: 10px; height: 10px; background-color: #ccc;"></div><div style="width: 10px; height: 10px; background-color: #ccc;"></div><div style="width: 10px; height: 10px; background-color: #ccc;"></div><div style="width: 10px; height: 10px; background-color: #ccc;"></div><div style="width: 10px; height: 10px; background-color: #ccc;"></div><div style="width: 10px; height: 10px; background-color: #ccc;"></div><div style="width: 10px; height: 10px; background-color: #ccc;"></div><div style="width: 10px; height: 10px; background-color: #ccc;"></div><div style="width: 10px; height: 10px; background-color: #ccc;"></div><div style="width: 10px; height: 10px; background-color: #ccc;"></div><div style="width: 10px; height: 10px; background-color: #ccc;"></div></div>	  
<a href="#">check power on</a>	Job Template	<div style="display: flex; gap: 2px;"><div style="width: 10px; height: 10px; background-color: #dc3545;"></div><div style="width: 10px; height: 10px; background-color: #28a745;"></div><div style="width: 10px; height: 10px; background-color: #ccc;"></div><div style="width: 10px; height: 10px; background-color: #ccc;"></div><div style="width: 10px; height: 10px; background-color: #ccc;"></div><div style="width: 10px; height: 10px; background-color: #ccc;"></div><div style="width: 10px; height: 10px; background-color: #ccc;"></div><div style="width: 10px; height: 10px; background-color: #ccc;"></div><div style="width: 10px; height: 10px; background-color: #ccc;"></div><div style="width: 10px; height: 10px; background-color: #ccc;"></div><div style="width: 10px; height: 10px; background-color: #ccc;"></div><div style="width: 10px; height: 10px; background-color: #ccc;"></div><div style="width: 10px; height: 10px; background-color: #ccc;"></div><div style="width: 10px; height: 10px; background-color: #ccc;"></div><div style="width: 10px; height: 10px; background-color: #ccc;"></div><div style="width: 10px; height: 10px; background-color: #ccc;"></div><div style="width: 10px; height: 10px; background-color: #ccc;"></div><div style="width: 10px; height: 10px; background-color: #ccc;"></div><div style="width: 10px; height: 10px; background-color: #ccc;"></div></div>	  
<a href="#">evaluate from technical state</a>	Job Template	<div style="display: flex; gap: 2px;"><div style="width: 10px; height: 10px; background-color: #dc3545;"></div><div style="width: 10px; height: 10px; background-color: #28a745;"></div><div style="width: 10px; height: 10px; background-color: #28a745;"></div><div style="width: 10px; height: 10px; background-color: #ccc;"></div><div style="width: 10px; height: 10px; background-color: #ccc;"></div><div style="width: 10px; height: 10px; background-color: #ccc;"></div><div style="width: 10px; height: 10px; background-color: #ccc;"></div><div style="width: 10px; height: 10px; background-color: #ccc;"></div><div style="width: 10px; height: 10px; background-color: #ccc;"></div><div style="width: 10px; height: 10px; background-color: #ccc;"></div><div style="width: 10px; height: 10px; background-color: #ccc;"></div><div style="width: 10px; height: 10px; background-color: #ccc;"></div><div style="width: 10px; height: 10px; background-color: #ccc;"></div><div style="width: 10px; height: 10px; background-color: #ccc;"></div><div style="width: 10px; height: 10px; background-color: #ccc;"></div><div style="width: 10px; height: 10px; background-color: #ccc;"></div><div style="width: 10px; height: 10px; background-color: #ccc;"></div><div style="width: 10px; height: 10px; background-color: #ccc;"></div><div style="width: 10px; height: 10px; background-color: #ccc;"></div></div>	  
<a href="#">firmware inventory</a>	Job Template	<div style="display: flex; gap: 2px;"><div style="width: 10px; height: 10px; background-color: #28a745;"></div><div style="width: 10px; height: 10px; background-color: #28a745;"></div><div style="width: 10px; height: 10px; background-color: #28a745;"></div><div style="width: 10px; height: 10px; background-color: #ccc;"></div><div style="width: 10px; height: 10px; background-color: #ccc;"></div><div style="width: 10px; height: 10px; background-color: #ccc;"></div><div style="width: 10px; height: 10px; background-color: #ccc;"></div><div style="width: 10px; height: 10px; background-color: #ccc;"></div><div style="width: 10px; height: 10px; background-color: #ccc;"></div><div style="width: 10px; height: 10px; background-color: #ccc;"></div><div style="width: 10px; height: 10px; background-color: #ccc;"></div><div style="width: 10px; height: 10px; background-color: #ccc;"></div><div style="width: 10px; height: 10px; background-color: #ccc;"></div><div style="width: 10px; height: 10px; background-color: #ccc;"></div><div style="width: 10px; height: 10px; background-color: #ccc;"></div><div style="width: 10px; height: 10px; background-color: #ccc;"></div><div style="width: 10px; height: 10px; background-color: #ccc;"></div><div style="width: 10px; height: 10px; background-color: #ccc;"></div><div style="width: 10px; height: 10px; background-color: #ccc;"></div></div>	  
<a href="#">FRU</a>	Job Template	<div style="display: flex; gap: 2px;"><div style="width: 10px; height: 10px; background-color: #28a745;"></div><div style="width: 10px; height: 10px; background-color: #ccc;"></div><div style="width: 10px; height: 10px; background-color: #ccc;"></div><div style="width: 10px; height: 10px; background-color: #ccc;"></div><div style="width: 10px; height: 10px; background-color: #ccc;"></div><div style="width: 10px; height: 10px; background-color: #ccc;"></div><div style="width: 10px; height: 10px; background-color: #ccc;"></div><div style="width: 10px; height: 10px; background-color: #ccc;"></div><div style="width: 10px; height: 10px; background-color: #ccc;"></div><div style="width: 10px; height: 10px; background-color: #ccc;"></div><div style="width: 10px; height: 10px; background-color: #ccc;"></div><div style="width: 10px; height: 10px; background-color: #ccc;"></div><div style="width: 10px; height: 10px; background-color: #ccc;"></div><div style="width: 10px; height: 10px; background-color: #ccc;"></div><div style="width: 10px; height: 10px; background-color: #ccc;"></div><div style="width: 10px; height: 10px; background-color: #ccc;"></div><div style="width: 10px; height: 10px; background-color: #ccc;"></div><div style="width: 10px; height: 10px; background-color: #ccc;"></div><div style="width: 10px; height: 10px; background-color: #ccc;"></div></div>	  
<a href="#">get logs</a>	Job Template	<div style="display: flex; gap: 2px;"><div style="width: 10px; height: 10px; background-color: #28a745;"></div><div style="width: 10px; height: 10px; background-color: #ccc;"></div><div style="width: 10px; height: 10px; background-color: #ccc;"></div><div style="width: 10px; height: 10px; background-color: #ccc;"></div><div style="width: 10px; height: 10px; background-color: #ccc;"></div><div style="width: 10px; height: 10px; background-color: #ccc;"></div><div style="width: 10px; height: 10px; background-color: #ccc;"></div><div style="width: 10px; height: 10px; background-color: #ccc;"></div><div style="width: 10px; height: 10px; background-color: #ccc;"></div><div style="width: 10px; height: 10px; background-color: #ccc;"></div><div style="width: 10px; height: 10px; background-color: #ccc;"></div><div style="width: 10px; height: 10px; background-color: #ccc;"></div><div style="width: 10px; height: 10px; background-color: #ccc;"></div><div style="width: 10px; height: 10px; background-color: #ccc;"></div><div style="width: 10px; height: 10px; background-color: #ccc;"></div><div style="width: 10px; height: 10px; background-color: #ccc;"></div><div style="width: 10px; height: 10px; background-color: #ccc;"></div><div style="width: 10px; height: 10px; background-color: #ccc;"></div><div style="width: 10px; height: 10px; background-color: #ccc;"></div></div>	  
<a href="#">power off</a>	Job Template	<div style="display: flex; gap: 2px;"><div style="width: 10px; height: 10px; background-color: #28a745;"></div><div style="width: 10px; height: 10px; background-color: #28a745;"></div><div style="width: 10px; height: 10px; background-color: #ccc;"></div><div style="width: 10px; height: 10px; background-color: #ccc;"></div><div style="width: 10px; height: 10px; background-color: #ccc;"></div><div style="width: 10px; height: 10px; background-color: #ccc;"></div><div style="width: 10px; height: 10px; background-color: #ccc;"></div><div style="width: 10px; height: 10px; background-color: #ccc;"></div><div style="width: 10px; height: 10px; background-color: #ccc;"></div><div style="width: 10px; height: 10px; background-color: #ccc;"></div><div style="width: 10px; height: 10px; background-color: #ccc;"></div><div style="width: 10px; height: 10px; background-color: #ccc;"></div><div style="width: 10px; height: 10px; background-color: #ccc;"></div><div style="width: 10px; height: 10px; background-color: #ccc;"></div><div style="width: 10px; height: 10px; background-color: #ccc;"></div><div style="width: 10px; height: 10px; background-color: #ccc;"></div><div style="width: 10px; height: 10px; background-color: #ccc;"></div><div style="width: 10px; height: 10px; background-color: #ccc;"></div><div style="width: 10px; height: 10px; background-color: #ccc;"></div></div>	  

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

**firmware inventory** ✕

DETAILS PERMISSIONS NOTIFICATIONS COMPLETED JOBS SCHEDULES ADD SURVEY

\* NAME  DESCRIPTION  \*JOB TYPE   PROMPT ON LAUNCH

\* INVENTORY   PROMPT ON LAUNCH \* PROJECT  \* PLAYBOOK

CREDENTIAL   PROMPT ON LAUNCH FORKS  LIMIT   PROMPT ON LAUNCH

\* VERBOSITY   PROMPT ON LAUNCH JOB TAGS   PROMPT ON LAUNCH SKIP TAGS   PROMPT ON LAUNCH

LABELS  INSTANCE GROUPS  JOB SLICING

TIMEOUT  SHOW CHANGES   PROMPT ON LAUNCH

OPTIONS  
 ENABLE PRIVILEGE ESCALATION  ALLOW PROVISIONING CALLBACKS  
 ENABLE CONCURRENT JOBS  USE FACT CACHE

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.

JOBS / 33 - firmware inventory

**DETAILS**

STATUS ● Successful

STARTED 6/21/2019 6:01:36 PM

FINISHED 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](#)

INSTANCE GROUP [tower](#)

EXTRA VARIABLES YAML JSON EXPAND

1 ---

firmware inventory

PLAYS 1 TASKS 6 HOSTS 1 ELAPSED 00:00:21

SEARCH Q KEY

```
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 PLAY [Firmware Update] 18:01:40
13 *****
14 META: ran handlers
15 TASK [Create Auth token] 18:01:40
16 *****
17 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.

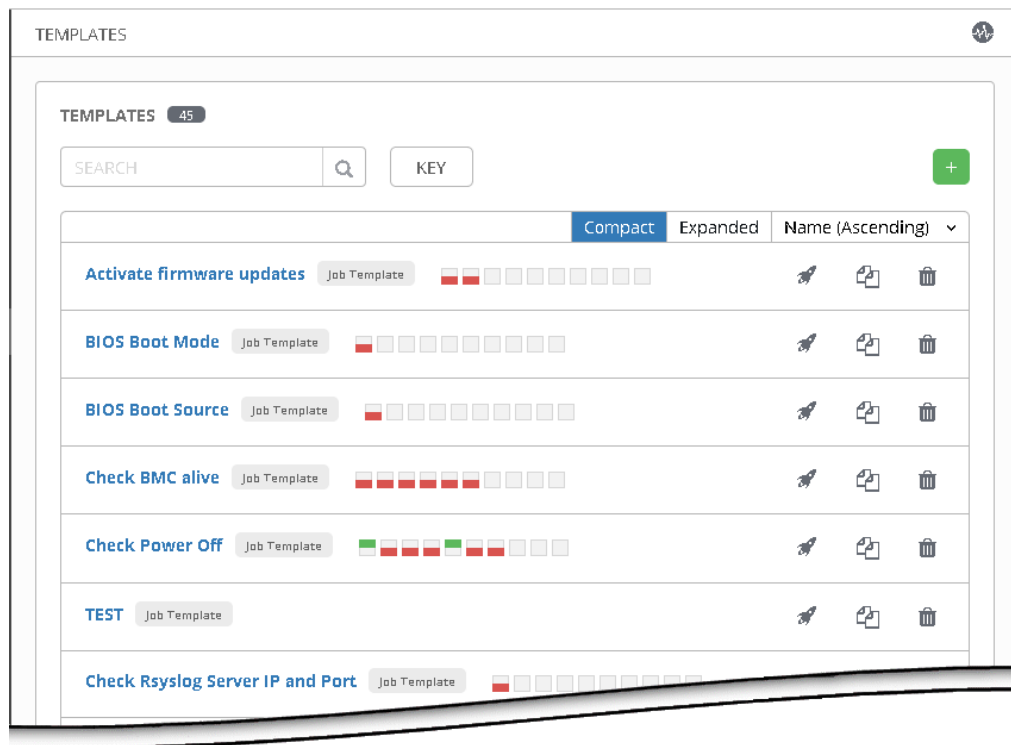
---

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

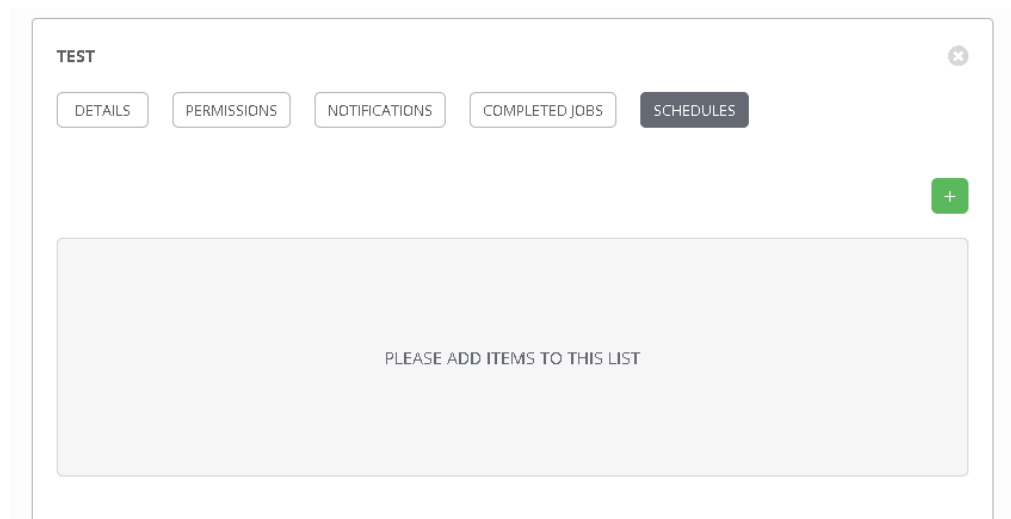
---

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

#### Templates example



2. Click a resource.



3. Click the **Schedules** tab.
4. Complete the fields as required.

### Example

**MySchedule**
✖

\* NAME

\* START DATE

\* START TIME (HH24:MM:SS)

 :  :

\* LOCAL TIME ZONE

\* REPEAT FREQUENCY

**FREQUENCY DETAILS**

\* EVERY

 MONTH  
S

\* ON DAY

\* ON THE

\* END

\* OCCURRENCES

**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

---

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

---

5. Click **Save** to complete changes.
- The schedule is created for the resource.

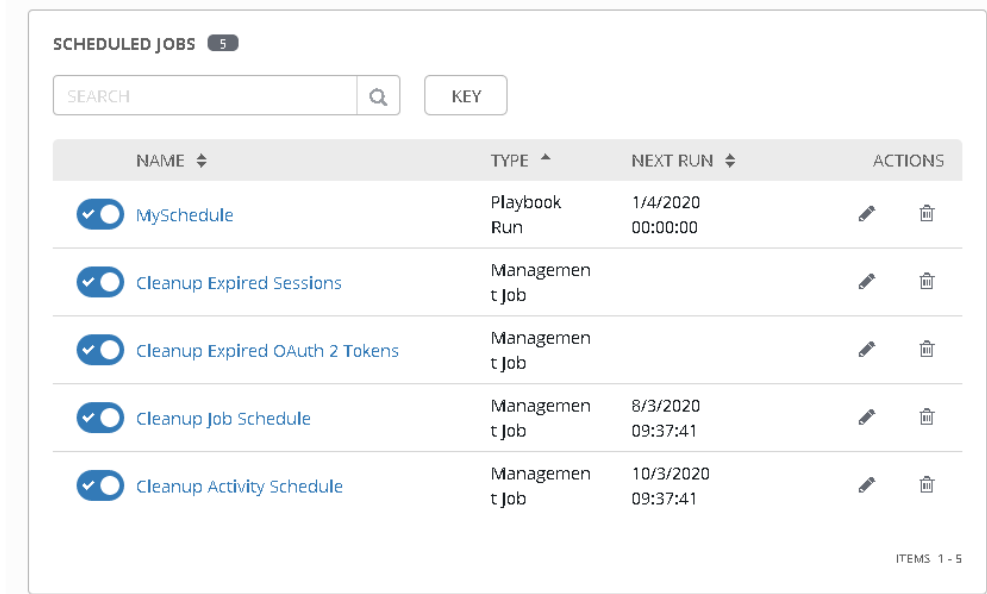
**TEST**
✖

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	<input type="button" value="✎"/> <input type="button" value="🗑"/>

ITEMS 1 - 1

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

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



The screenshot displays a web interface for managing scheduled jobs. At the top, it says "SCHEDULED JOBS" with a notification badge showing the number "5". Below this is a search bar with the placeholder text "SEARCH" and a magnifying glass icon, followed by a "KEY" button. The main content is a table with four columns: "NAME", "TYPE", "NEXT RUN", and "ACTIONS". Each row represents a scheduled job and includes a toggle switch on the left. The jobs listed are: "MySchedule" (Playbook Run, next run 1/4/2020 00:00:00), "Cleanup Expired Sessions" (Management Job), "Cleanup Expired OAuth 2 Tokens" (Management Job), "Cleanup Job Schedule" (Management Job, next run 8/3/2020 09:37:41), and "Cleanup Activity Schedule" (Management Job, next run 10/3/2020 09:37:41). The "ACTIONS" column for each job contains edit and delete icons. In the bottom right corner of the table area, it says "ITEMS 1 - 5".

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 several tabs: DETAILS (selected), 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:** Bull Sequana Edge Vault | bullsequana\_edge\_password
- FORKS:** 0
- LIMIT:** (empty)
- VERBOSITY:** 0 (Normal)
- JOB TAGS:** (empty)
- SKIP TAGS:** (empty)
- LABELS:** (empty)
- INSTANCE GROUPS:** (empty)
- JOB SLICING:** 1
- TIMEOUT:** 0
- SHOW CHANGES:** (toggle off)
- OPTIONS:**
  - ENABLE PRIVILEGE ESCALATION (checkbox off)
  - ALLOW PROVISIONING CALLBACKS (checkbox off)
  - ENABLE CONCURRENT JOBS (checkbox off)
  - USE FACT CACHE (checkbox off)

### 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 "KEY" button. A table lists the credentials:

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 two tabs: DETAILS (selected) and PERMISSIONS. The configuration includes:

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

CANCEL SAVE

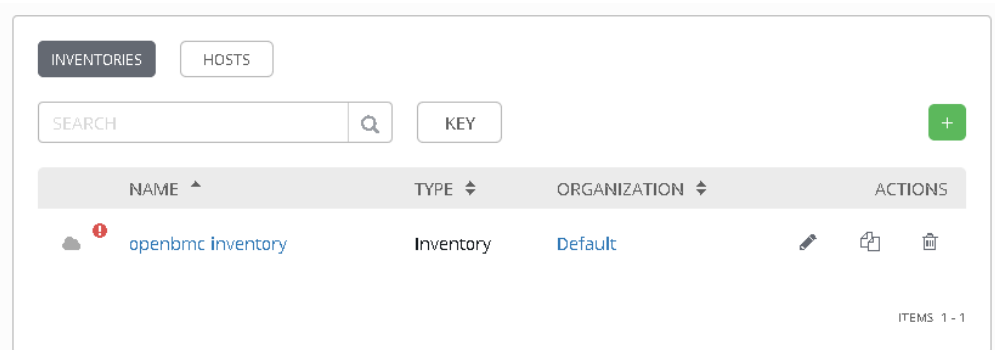
3. Complete the **Vault Password** field.
4. Click **Save**. The **Vault Password** field is now encrypted.

## 2.5.2. Creating an encrypted password for a host

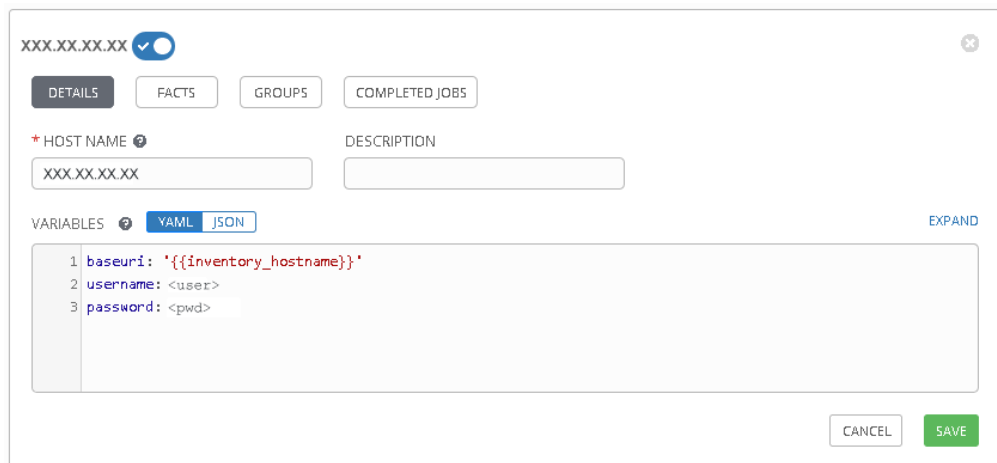
1. Choose a name for the password that is going to be encrypted.
2. Open a Terminal window.
3. Run the following command:

```
$. /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

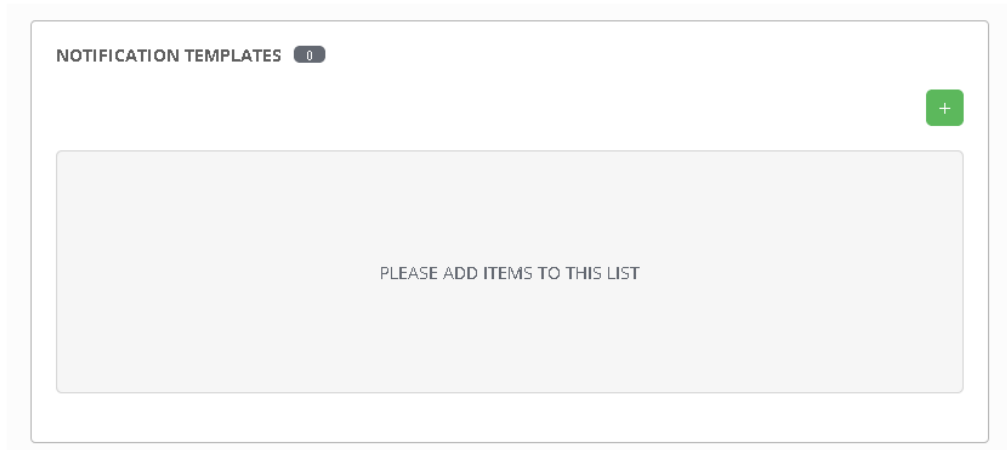
The encrypted passwords are stored in the `passwords.yml` file in the `/ansible/vars` sub-directory of the MISM installation directory. To delete one, perform the following actions:

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

**NEW NOTIFICATION TEMPLATE**

\* NAME: MyEmail      DESCRIPTION:      \* ORGANIZATION: Bull

\* TYPE: Email

**TYPE DETAILS**

USERNAME:      PASSWORD: SHOW      \* HOST: XXX.XX.X.XX

\* RECIPIENT LIST: YY.YY@atos.net      \* SENDER EMAIL: XX.XX@atos.net      \* PORT: 25

\* TIMEOUT: 30      OPTIONS:  USE TLS,  USE SSL

CUSTOMIZE MESSAGES...

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.

6. Click **Save** to complete changes.

The notification template is created.

**NOTIFICATION TEMPLATES** 1

SEARCH      KEY      +

NAME	TYPE	ACTIONS
MyEmail	Email	

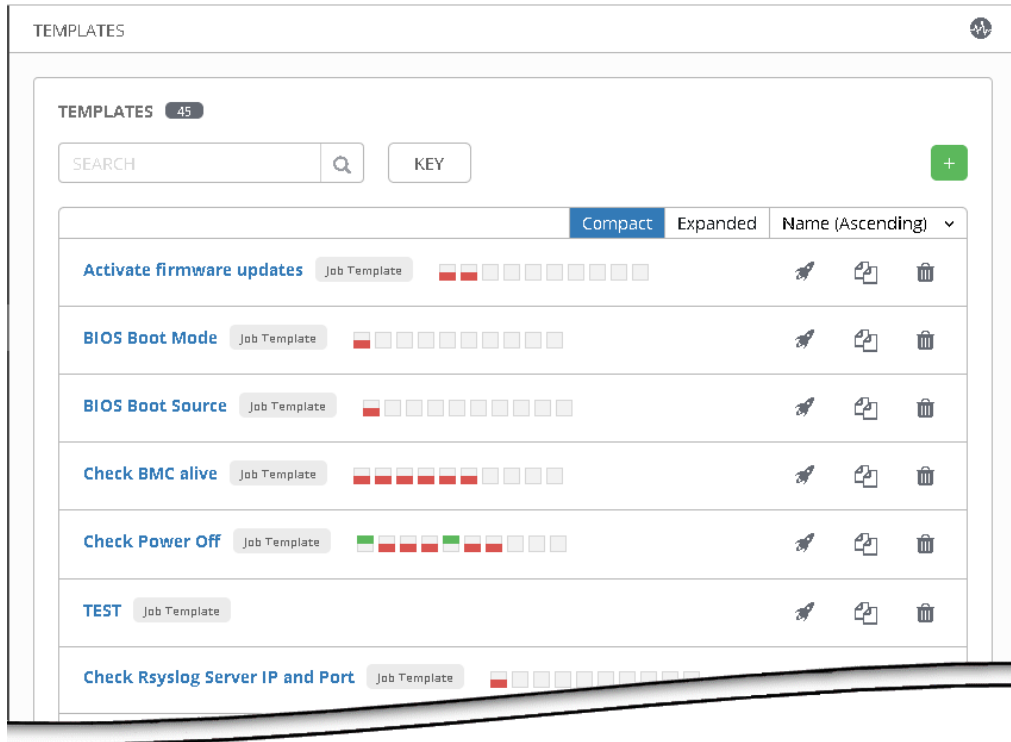
ITEMS 1 - 1

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

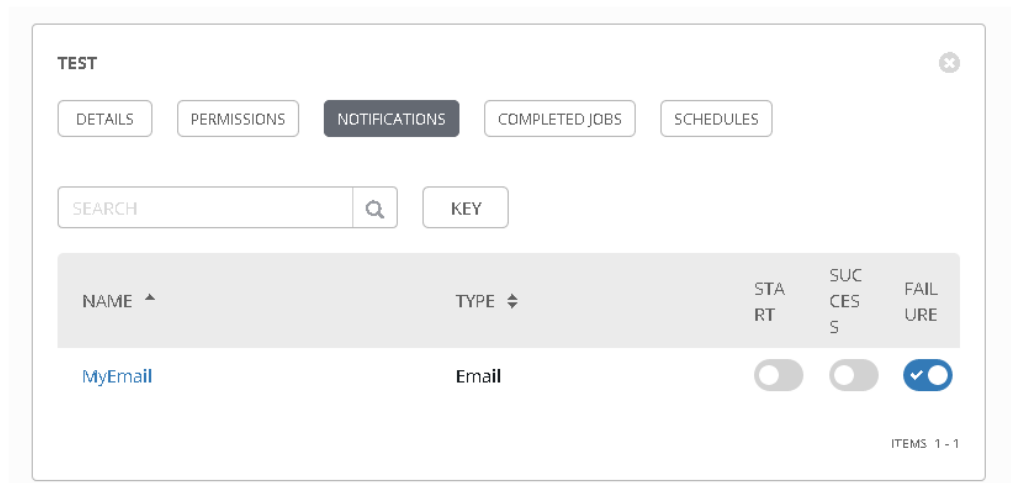
## 2.6.2. Assigning a notification to a job template

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 immediate reboot and shutdown buttons should only be used if the Operating System is unable to respond to an orderly reboot or 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 BMCs

---

**Important** The date and time will be lost following a BMC reboot if they have been set manually. It is recommended to use NTP to set the date and time to preserve the settings when the BMC is rebooted.

---

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' (containing 'My first inventory'), 'DESCRIPTION', and '\* ORGANIZATION' (containing 'Default'). There are also search fields for 'INSIGHTS CREDENTIAL' and 'INSTANCE GROUPS'. A 'VARIABLES' section is expanded, showing a code editor with the following content:

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

At the bottom right of the variables section, there are 'CANCEL' and 'SAVE' buttons.

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>

---

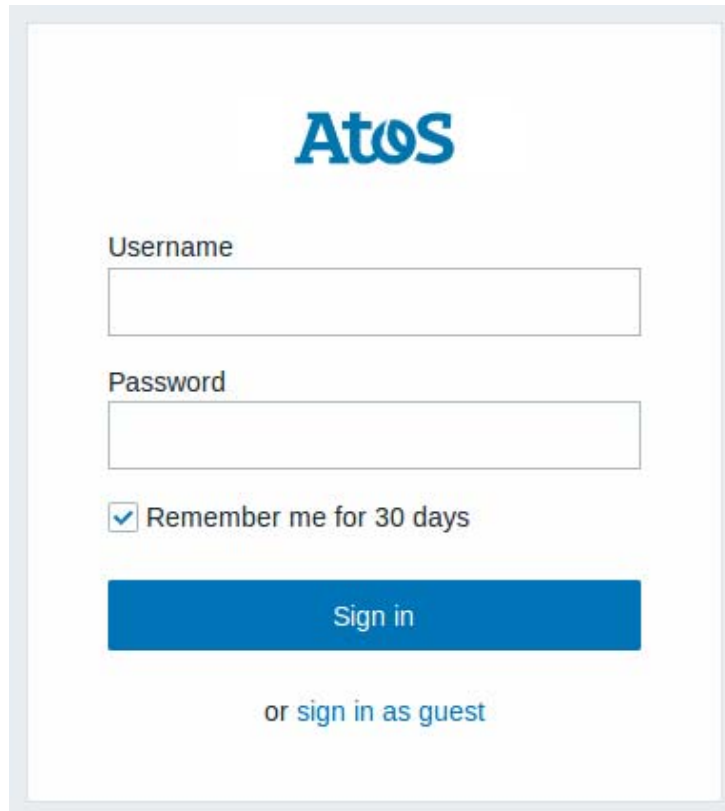
## 3.1. Logging in

### 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)

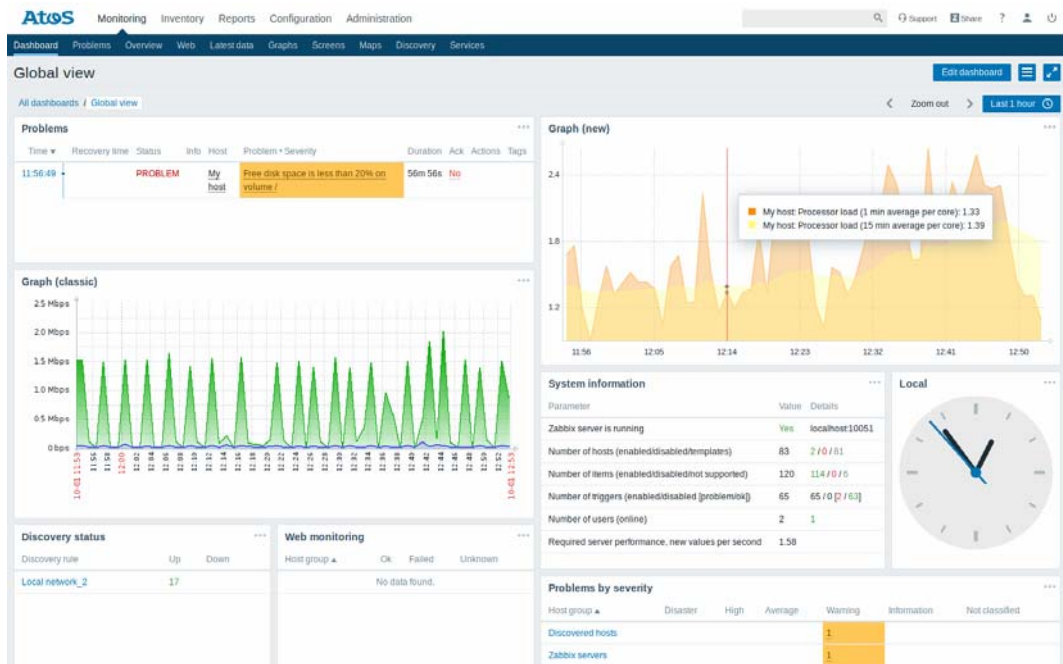
---

**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
Configuration	Allows to set up major functions: hosts and host groups, data gathering, data thresholds, sending problem notifications, creating data visualization and others.	Notifications
		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

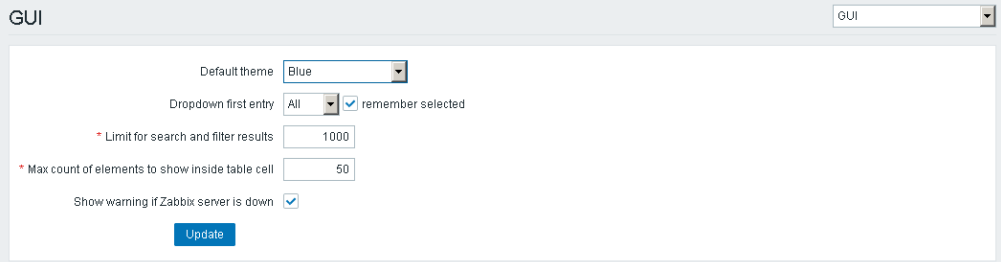
On delivery, the monitoring console contains two templates that allow Zabbix to be used to monitor BullSequana Edge servers:

- 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

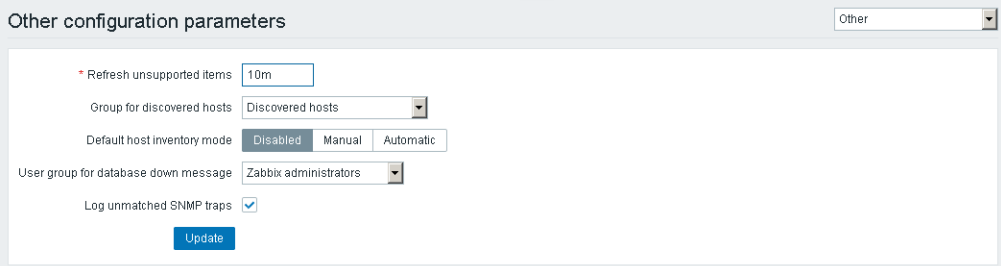
1. From the **Administration** menu, click the **General** tab. The **GUI** page opens.



The screenshot shows the 'GUI' configuration page. It features a title bar with 'GUI' and a dropdown menu. The main content area includes the following settings:

- Default theme: Blue (dropdown)
- Dropdown first entry: All (dropdown) with a checked checkbox for 'remember selected'
- \* Limit for search and filter results: 1000 (input field)
- \* Max count of elements to show inside table cell: 50 (input field)
- Show warning if Zabbix server is down: checked checkbox
- Update button

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



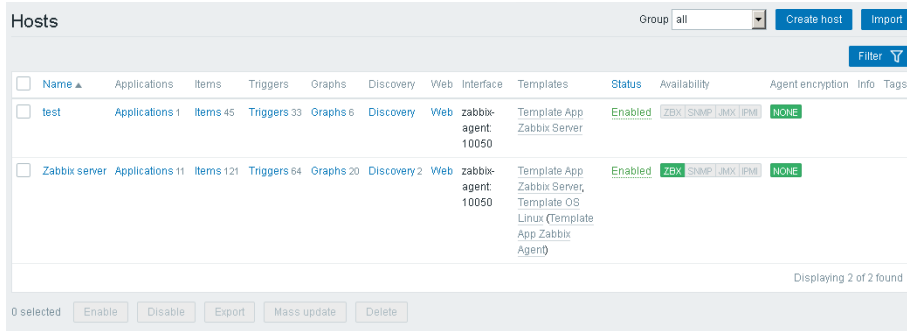
The screenshot shows the 'Other configuration parameters' page. It features a title bar with 'Other' and a dropdown menu. The main content area includes the following settings:

- \* Refresh unsupported items: 10m (input field)
- Group for discovered hosts: Discovered hosts (dropdown)
- Default host inventory mode: Disabled (radio button), Manual (radio button), Automatic (radio button)
- User group for database down message: Zabbix administrators (dropdown)
- Log unmatched SNMP traps: checked checkbox
- Update button

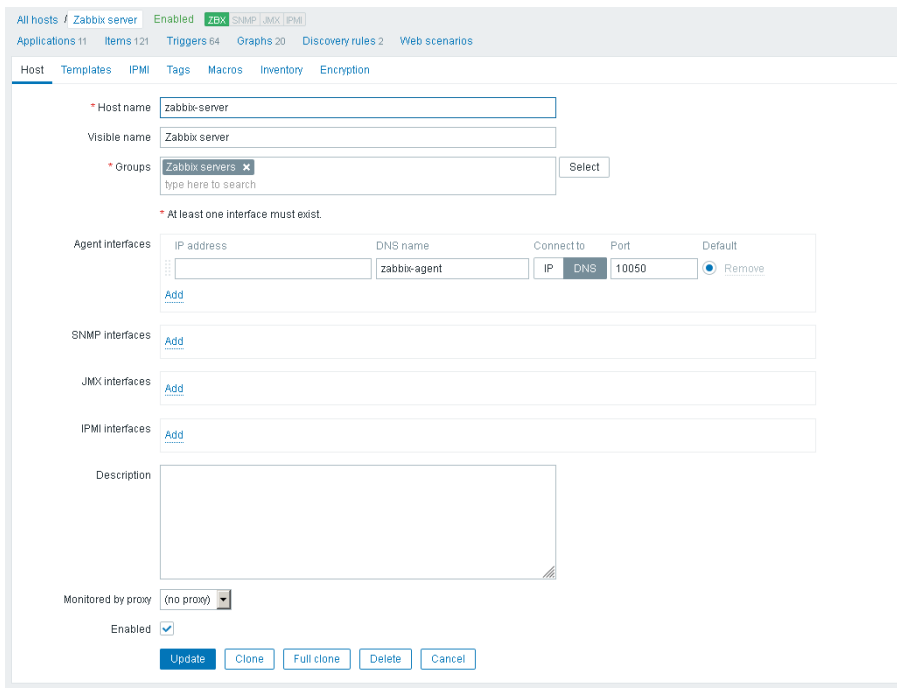
3. Click **Automatic** for **Default host inventory mode**.
4. Click **Update**.

### 3.3.2. Renaming the Zabbix server host

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



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



3. Complete the following fields.

Field	Value
Host name	zabbix-server
Visible name	Zabbix server

4. 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

5. Click **Update**.
6. Stop and restart the MISM console.

## 3.4. Managing the Atos LLD template

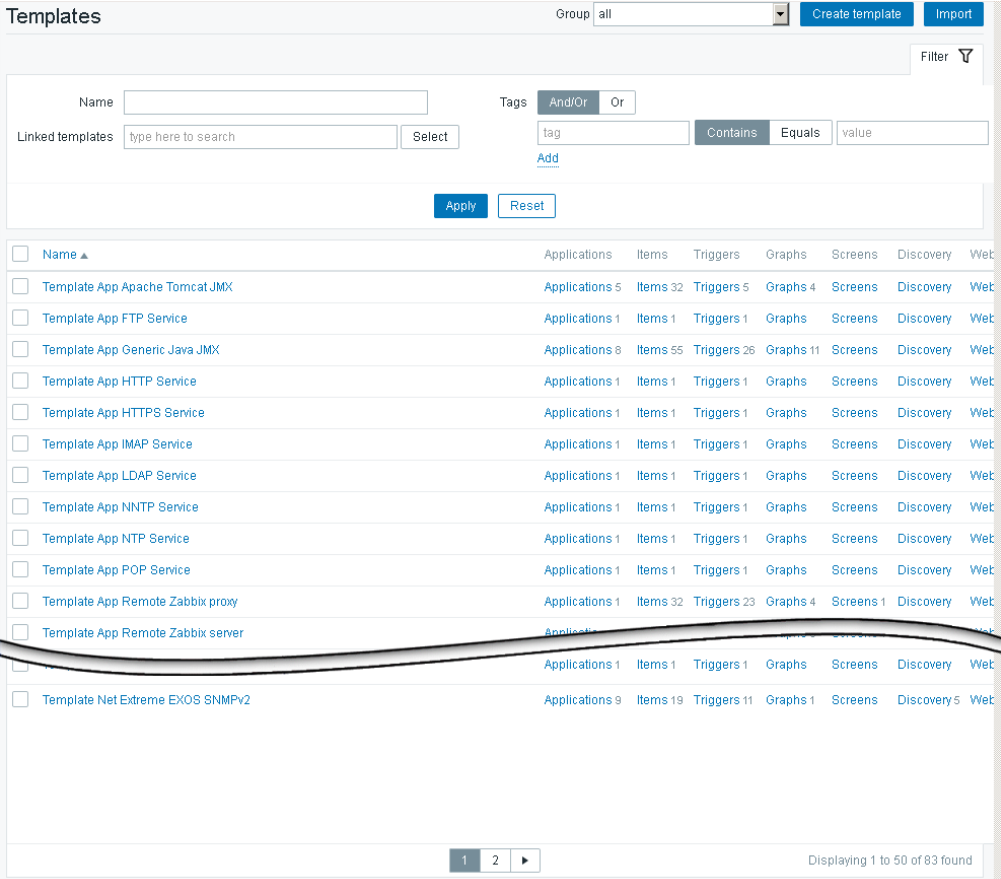
### 3.4.1. Template description

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 is a search bar for Name and a filter section with options for Tags (And/Or, Or) and a search box for tag, Contains, Equals, and value. Below the search bar, there are buttons for Apply and Reset. The main content is a table of templates with columns for Name, Applications, Items, Triggers, Graphs, Screens, Discovery, and Web.

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

At the bottom of the page, there is a pagination control showing '1 2' and a status message 'Displaying 1 to 50 of 83 found'.

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

Rules	Update existing	Create new	Delete missing
Groups	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input 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 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 installation directory: `\zabbix\server\externalscripts`. They can be copied to any local directory.

---

4. Click **Import**.

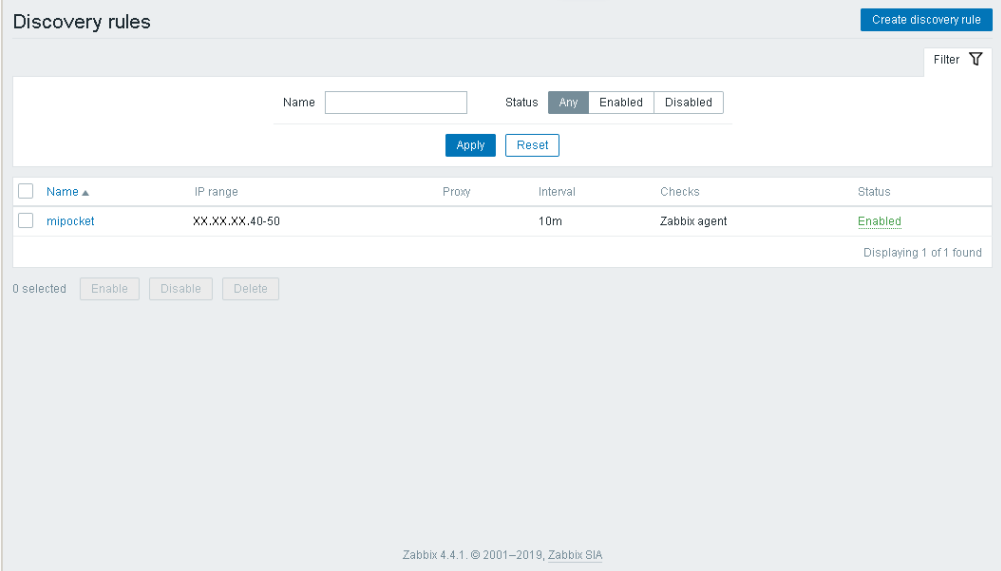


## 3.5. Adding resources

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

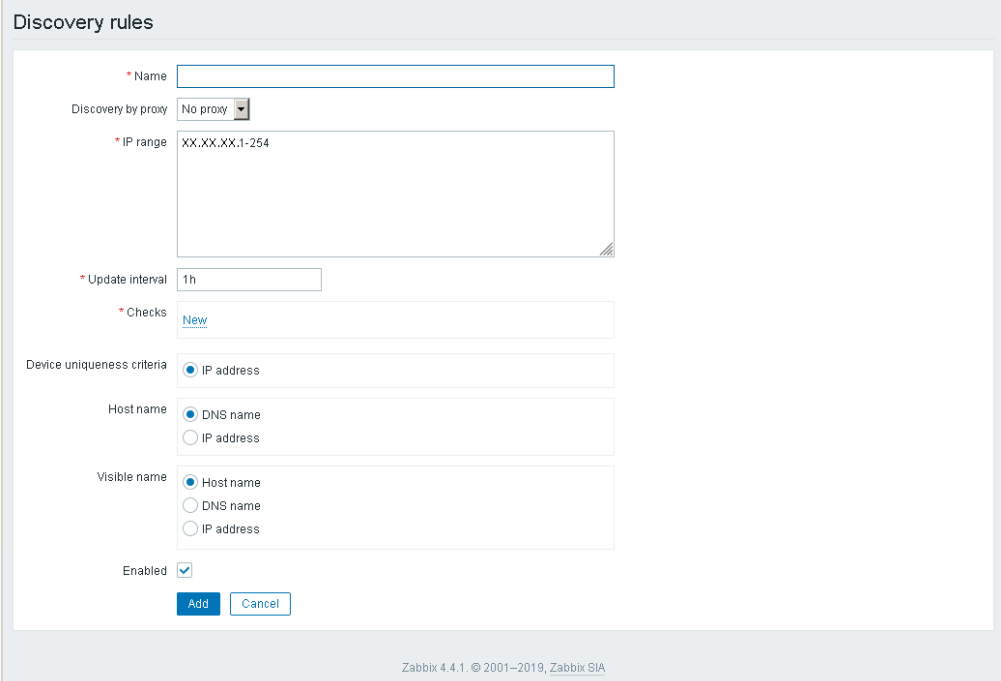
#### 3.5.1.1. Creating a discovery rule

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 the following 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' form. It includes the following fields and options: 'Name' (text input), 'Discovery by proxy' (dropdown menu set to 'No proxy'), 'IP range' (text input with 'XX.XX.XX.1-254'), 'Update interval' (text input with '1h'), 'Checks' (text input with 'New'), 'Device uniqueness criteria' (radio buttons for 'IP address'), 'Host name' (radio buttons for 'DNS name' and 'IP address'), 'Visible name' (radio buttons for 'Host name', 'DNS name', and 'IP address'), and an 'Enabled' checkbox. 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

Discovery rules

\* Name

Discovery by proxy

\* IP range

\* Update interval

\* Checks [New](#)

Check type

\* Port range

[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

Discovery rule created

Discovery rules [Create discovery rule](#)

Name  Status

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

<input type="checkbox"/>	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

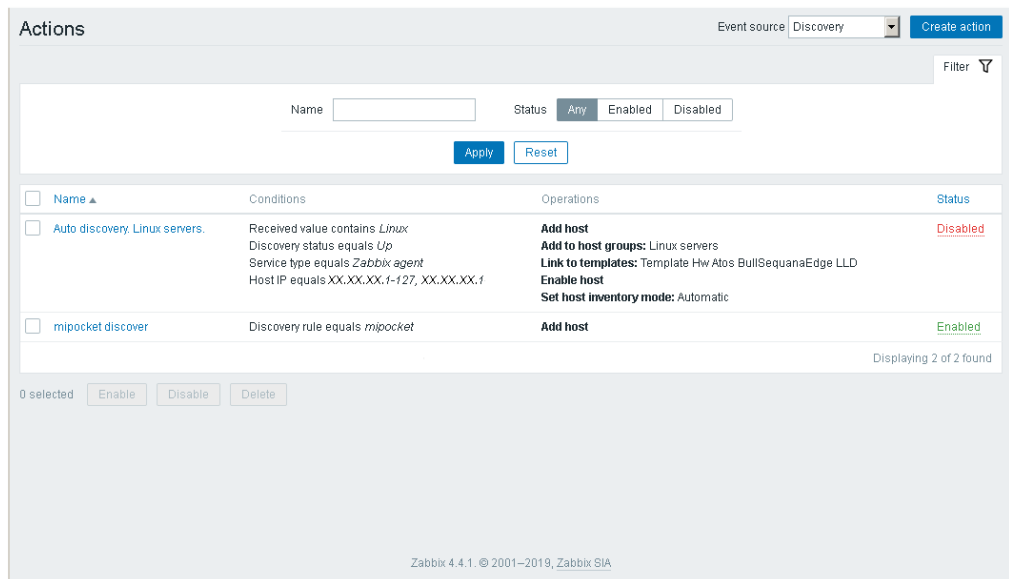
0 selected [Enable](#) [Disable](#) [Delete](#)

Displaying 2 of 2 found

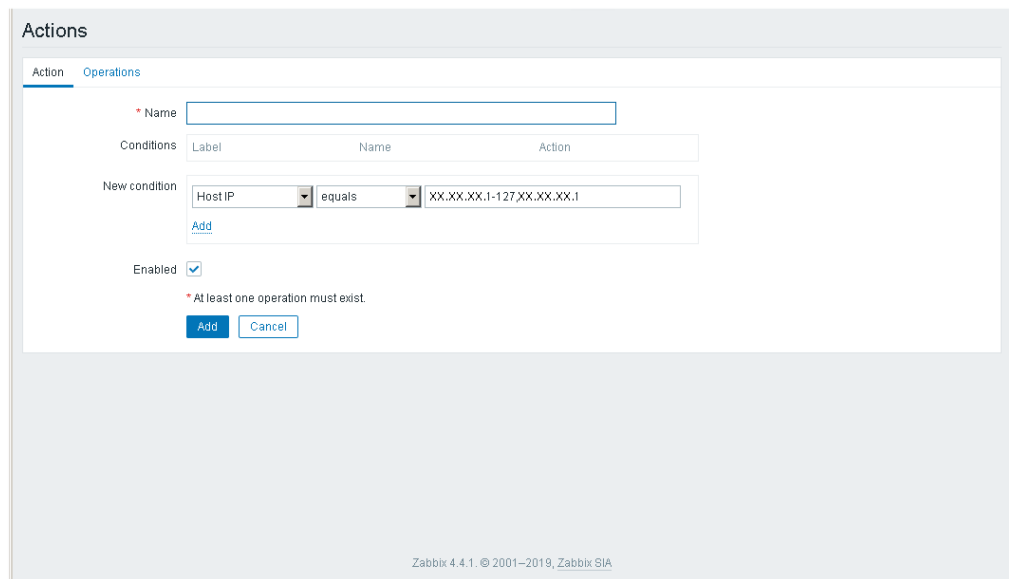
Zabbix 4.4.1. © 2001–2019, Zabbix SIA

### 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.



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



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

The screenshot shows the 'Actions' configuration page in Zabbix, specifically the 'Operations' tab. The page has a header with 'Action' and 'Operations' tabs. Below the header, there is a form with the following elements:

- A required text field for 'Name'.
- A table for 'Conditions' with columns 'Label', 'Name', and 'Action'.
- A 'New condition' section with a dropdown for 'Discovery rule', a dropdown for 'equals', a search box containing 'MyMipockets', and a 'Select' button.
- An 'Add' button below the search box.
- An 'Enabled' checkbox that is checked.
- A warning message: '\* At least one operation must exist'.
- 'Add' and 'Cancel' buttons at the bottom.

At the bottom of the page, the text 'Zabbix 4.4.1. © 2001–2019, Zabbix SIA' is visible.

## 4. 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 with 'Action' and 'Operations' tabs. Below the header, there is a form with the following elements:

- 'Default subject' field containing: 'Discovery: (DISCOVERY.DEVICE.STATUS) (DISCOVERY.DEVICE.IPADDRESS)'.
- 'Default message' field containing a list of variables: '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)'.
- 'Operations' section with a 'Details' tab and a 'New' button.
- A warning message: '\* At least one operation must exist'.
- 'Add' and 'Cancel' buttons at the bottom.

At the bottom of the page, the text 'Zabbix 4.4.1. © 2001–2019, Zabbix SIA' is visible.

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

Action Operations

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

Default message: {DISCOVERYRULE.NAME}  
{DISCOVERYDEVICE.IPADDRESS}  
{DISCOVERYDEVICE.DNS}  
{DISCOVERYDEVICE.STATUS}  
{DISCOVERYDEVICE.UPTIME}  
{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

Actions

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}`.

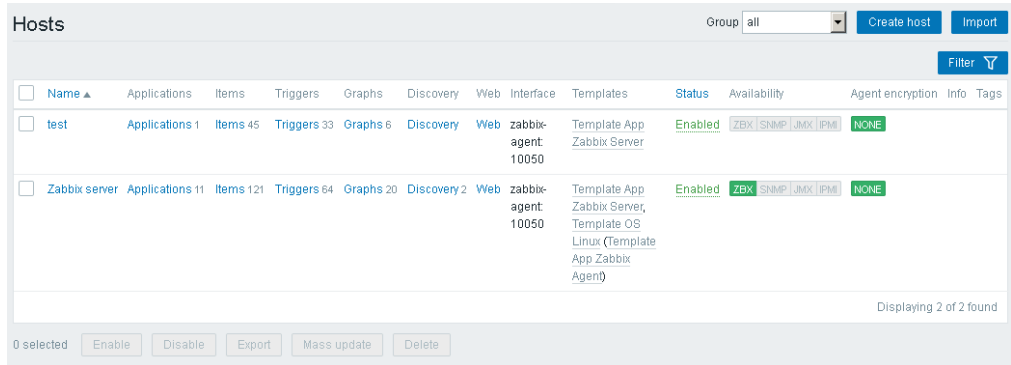
---

**See** 3.5.4. Filling Atos template macros

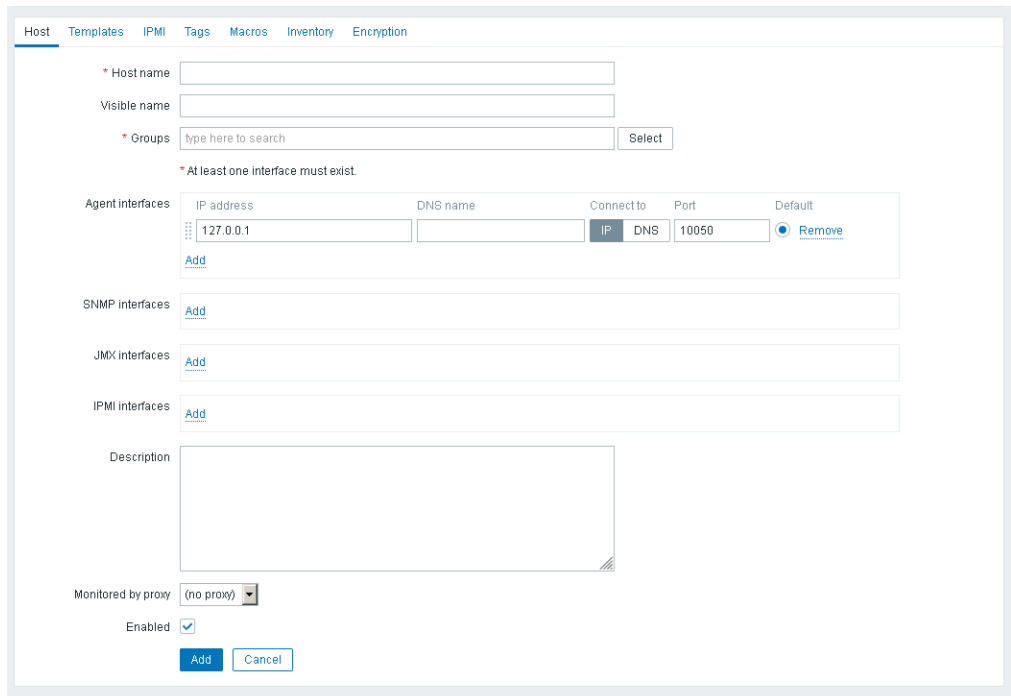
---

### 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 is divided into several sections: Host name, Visible name, Groups, Agent interfaces, SNMP interfaces, JMX interfaces, IPMI interfaces, Description, Monitored by proxy, and Enabled. The 'Agent interfaces' section is currently active, showing a table with columns for IP address, DNS name, Connect to, Port, and Default. The table contains one entry with IP address, DNS name 'zabbix-agent', and Port '10050'. The 'Enabled' checkbox is checked. At the bottom, there are buttons for 'Update', 'Clone', 'Full clone', 'Delete', and 'Cancel'.

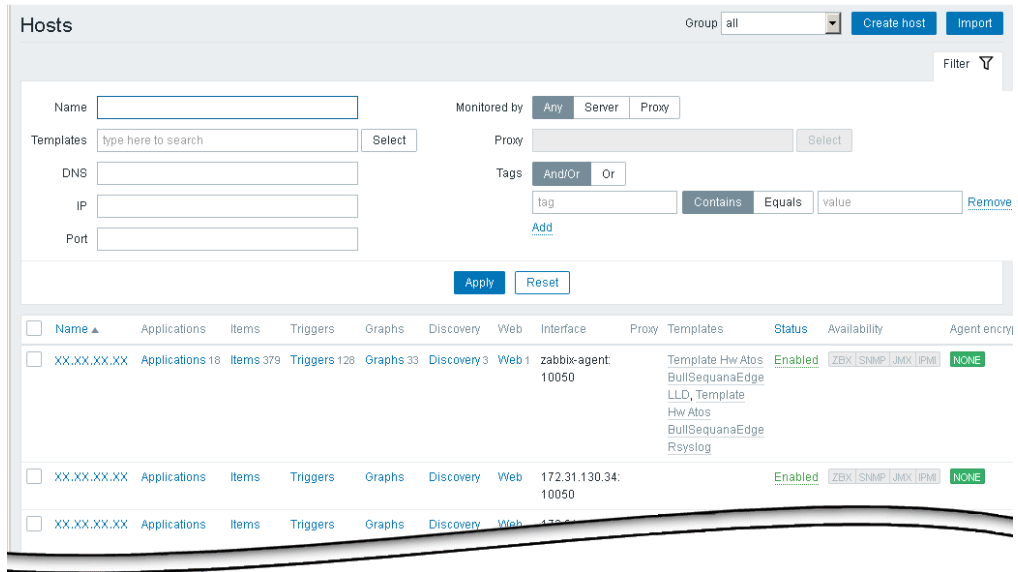
2. Click the **Template** tab above the host details. The host Template page opens.

The screenshot shows the Zabbix Host Template configuration page for the host 'test'. The page is divided into two main sections: 'Linked templates' and 'Link new templates'. The 'Linked templates' section shows a table with columns for Name and Action. The table contains one entry with Name 'Template App.Zabbix Server' and Action 'Unlink Unlink and clear'. The 'Link new templates' section has a search field 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 LLD template.
4. Click **Add**. The Atos LLD template appears in the **Linked templates** section.
5. Click **Update**.

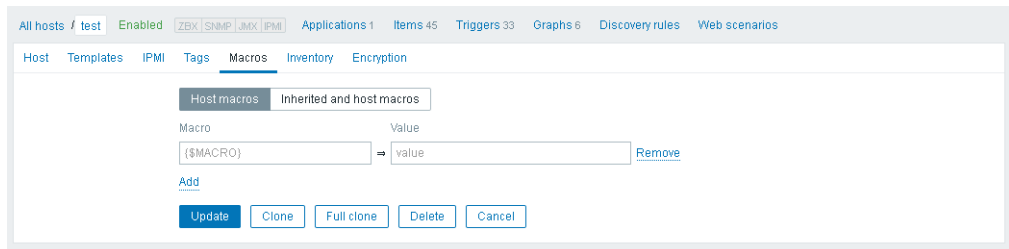
### 3.5.4. Filling Atos template macros

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 interface for configuring macros for a specific host. The host is 172.31.130.34 and is enabled. The 'Macros' tab is active, showing a table of macros. The table has three columns: Macro, Value, and Description. There are three rows of macros, each with a 'Remove' button. Below the table are buttons for 'Add', 'Update', 'Clone', 'Full clone', 'Delete', and 'Cancel'. The 'Update' button is highlighted in blue.

Macro	Value	Description
{\$OPENBMC}	XX.XX.XX.XX	description
{\$PASSWORD}	mypassword@gato	description
{\$USER}	root	description

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.

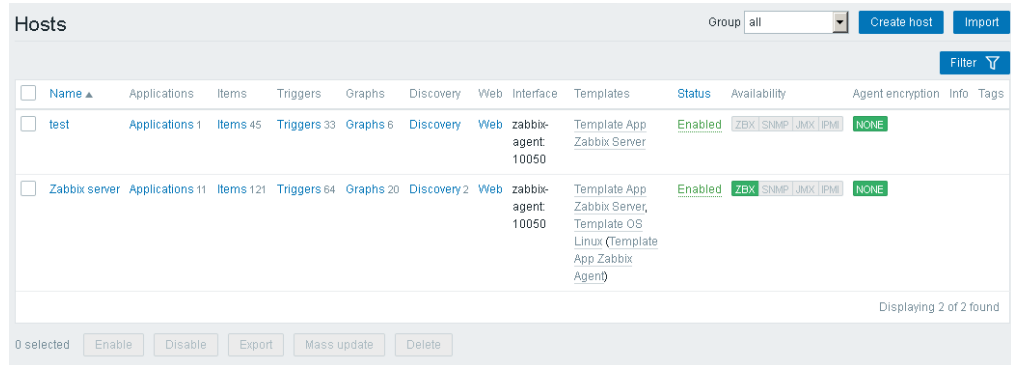
4. Go to the `/etc/zabbix/agent/` directory and open the `zabbix_agentd.conf` file with a text editor.
5. In the `TLS-RELATED PARAMETERS` section of the file, uncomment the following lines:

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

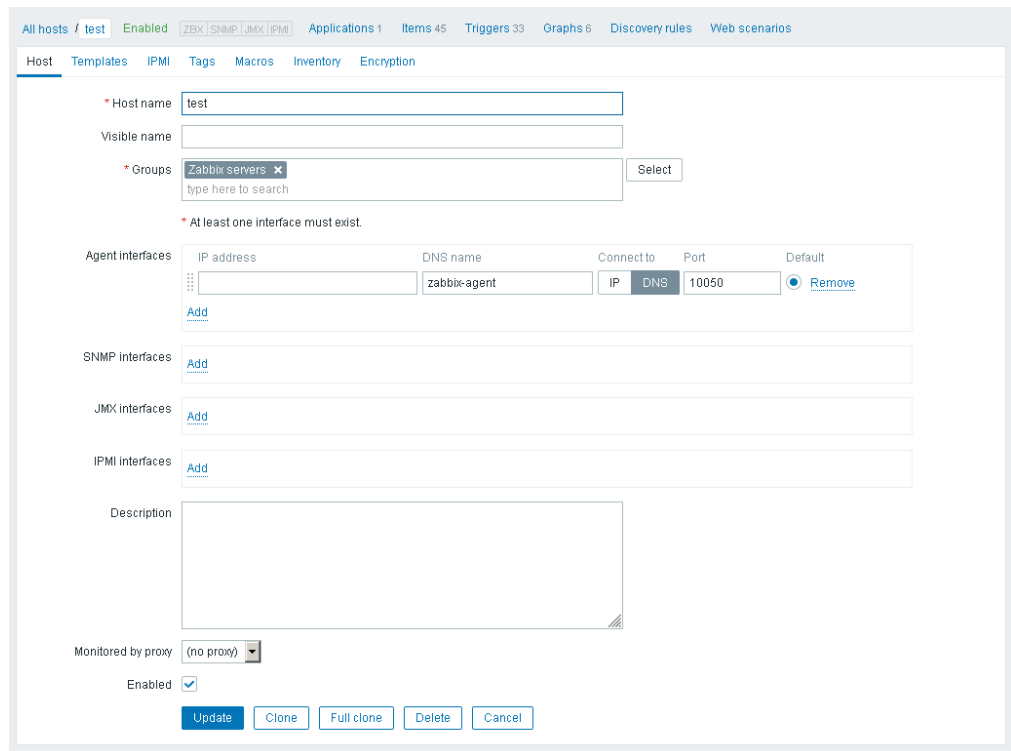
6. Save and close the file.
7. Stop and restart the MISM console.

### 3.6.2. Enabling PSK security for a host

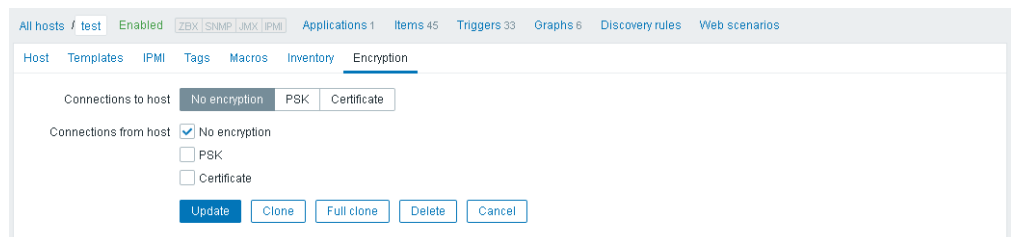
1. From the **Configuration** menu, click the **Hosts** tab. The **Hosts** page opens.



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



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



4. In the Connections to host section, click PSK.
5. In the Connections from host, select PSK.

6. Complete the following fields.

Field	Value
PSK Identity	PSK_Mipocket_Agent
echo PSK	Encryption key from the <code>zabbix_agentd.psk</code> file

7. Click **Update**.

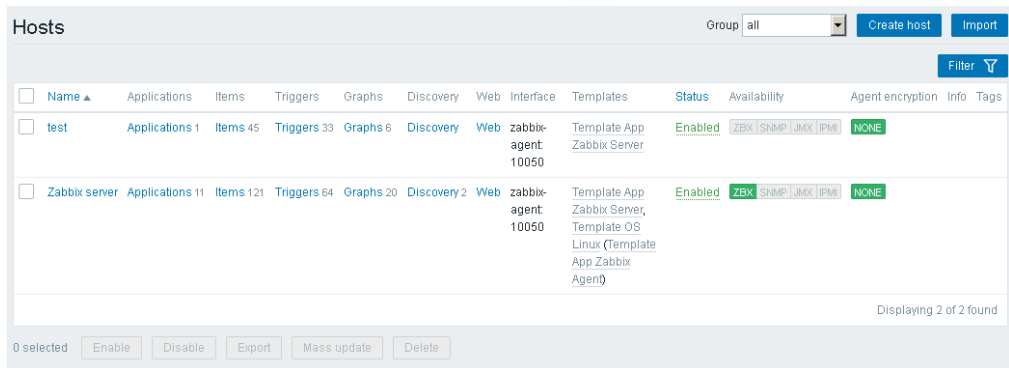
8. Stop and restart the MISM console.

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

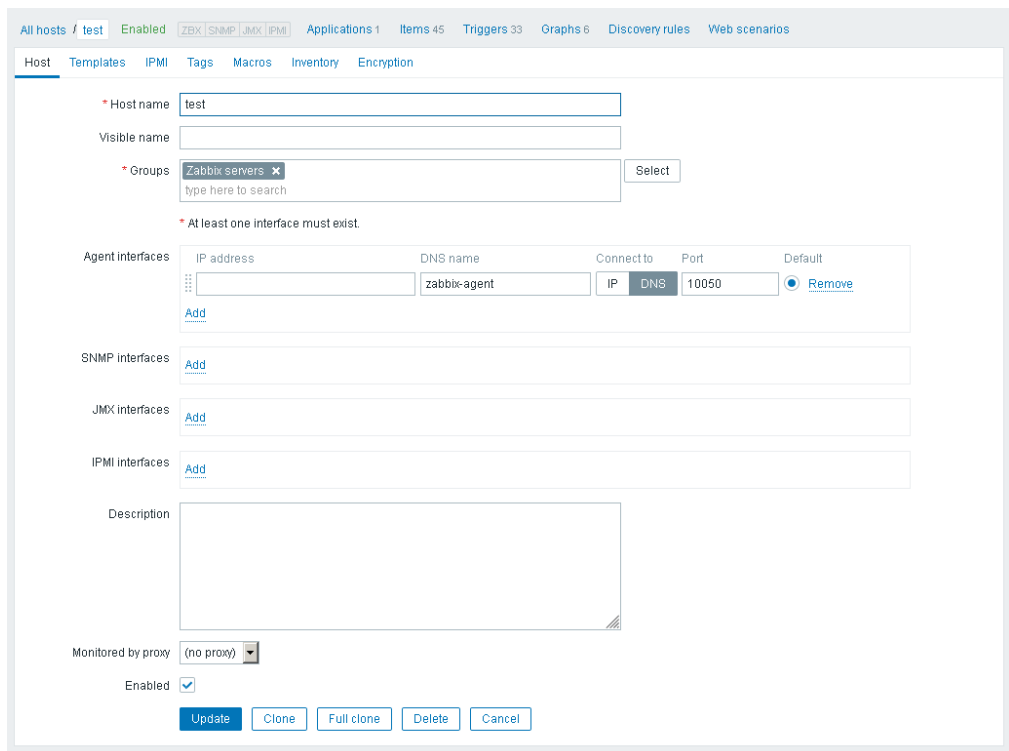
1. Go the MISM installation directory.
2. Generate an encrypted password using the following command:

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

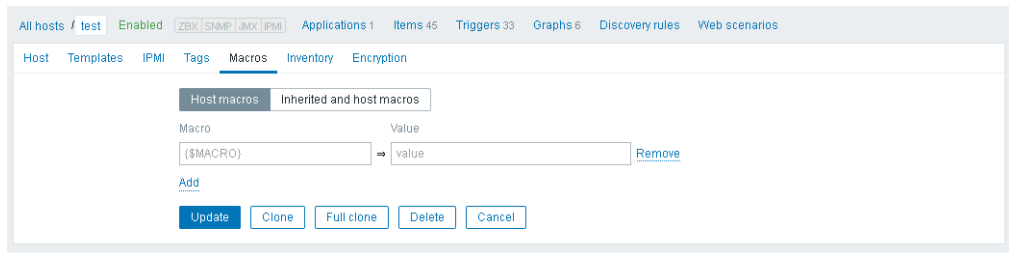
3. Copy the encrypted password.
4. From the **Configuration** menu, click the **Hosts** tab. The **Hosts** page opens.



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



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

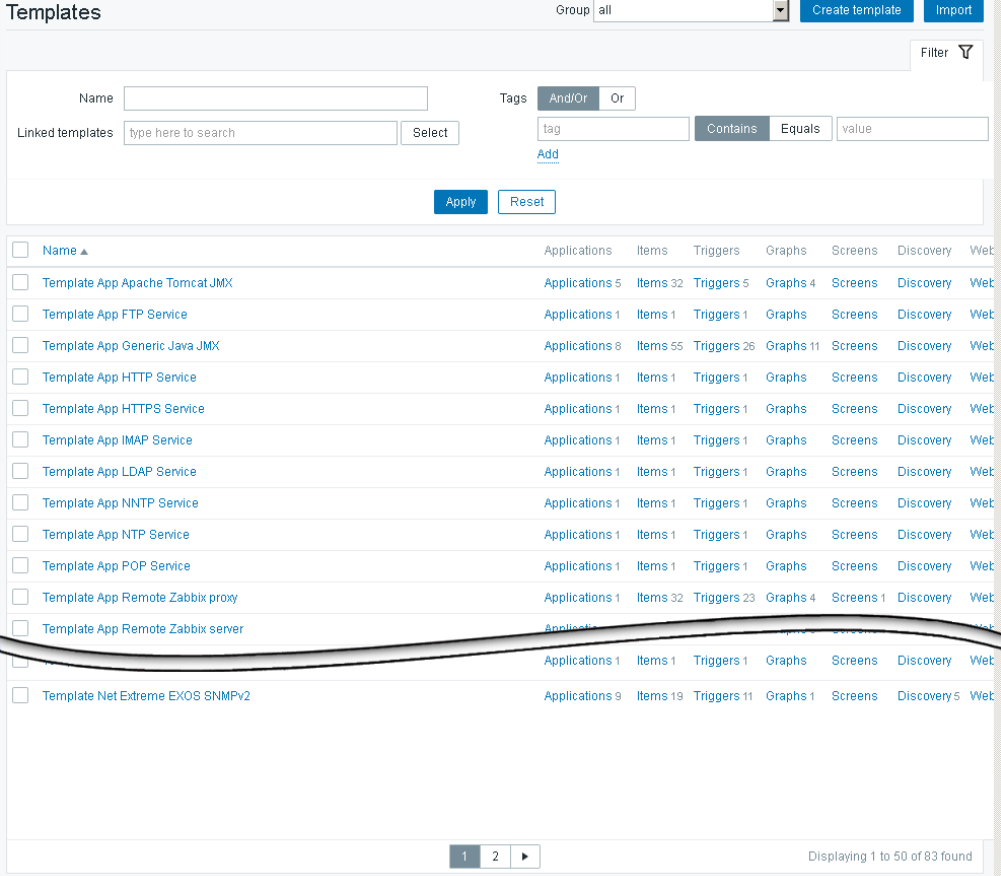


7. Paste the encrypted password in the **Value** field of the **{\$PASSWORD}** macro.
8. Click **Update**.

## 3.7. Enabling syslog forwarding

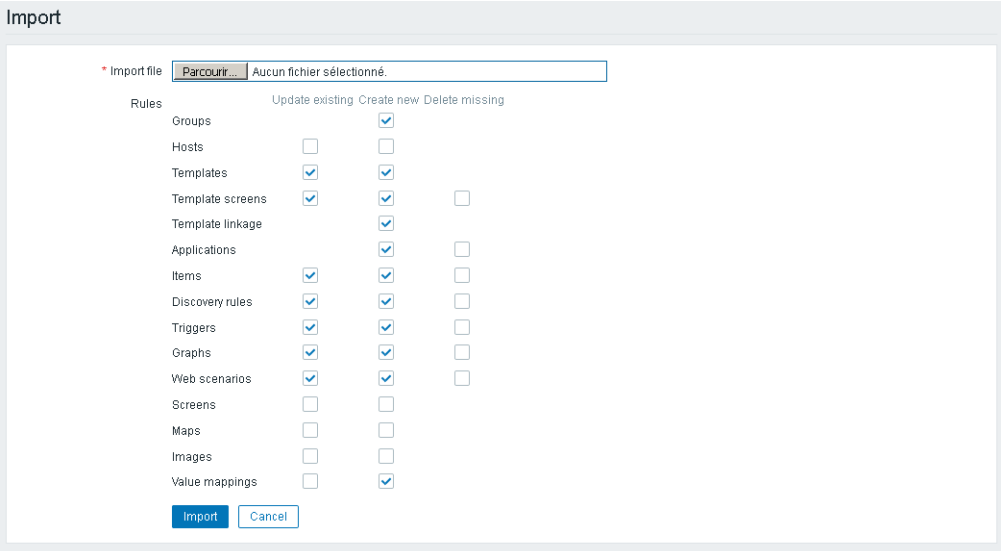
### 3.7.1. Importing the Atos Rsyslog template

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



The screenshot shows the Nagios Core 'Templates' page. At the top, there is a search bar and a 'Filter' button. Below that, there are fields for 'Name', 'Tags' (And/Or, Or), and 'Linked templates'. A table lists various templates, including 'Template App Remote Zabbix server' which is circled in red. The table columns are Name, Applications, Items, Triggers, Graphs, Screens, Discovery, and Web. At the bottom right, it says 'Displaying 1 to 50 of 83 found'.

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



The screenshot shows the Nagios Core 'Import' page. At the top, there is a section for 'Import file' with a 'Parcourir...' button and a text field containing 'Aucun fichier sélectionné.'. Below that, there are checkboxes for 'Rules' and 'Update existing'/'Create new'/'Delete missing' for various categories like 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.

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 Host configuration page for 'zabbix-server'. The page is titled 'All hosts / Zabbix server' and includes navigation links for Applications (11), Items (121), Triggers (64), Graphs (20), Discovery rules (2), and Web scenarios. The 'Host' tab is selected, and the configuration is for a 'Zabbix server' host. The 'Host name' is 'zabbix-server' and the 'Visible name' is 'Zabbix server'. The 'Groups' section shows 'Zabbix servers' selected. A note states '\* At least one interface must exist.' The 'Agent interfaces' section has one entry with IP address, DNS name 'zabbix-agent', Connect to 'IP', Port '10050', and Default selected. There are 'Add' buttons for Agent, SNMP, JMX, and IPMI interfaces. The 'Description' field is empty. The 'Monitored by proxy' is set to '(no proxy)' and 'Enabled' is 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 'zabbix-server'. The page is titled 'All hosts / Zabbix server' and includes navigation links for Applications (11), Items (121), Triggers (64), Graphs (20), Discovery rules (2), and Web scenarios. The 'Templates' tab is selected. The 'Linked templates' section shows two templates: 'Template App Zabbix Server' and 'Template OS Linux', each with 'Unlink' and 'Unlink and clear' actions. The 'Link new templates' section has a search box and a 'Select' button. There is an 'Add' button below the search box. 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 Rsyslog template.
4. Click **Add**. The Atos Rsyslog template appears in the **Linked templates** section.
5. Click **Update**.

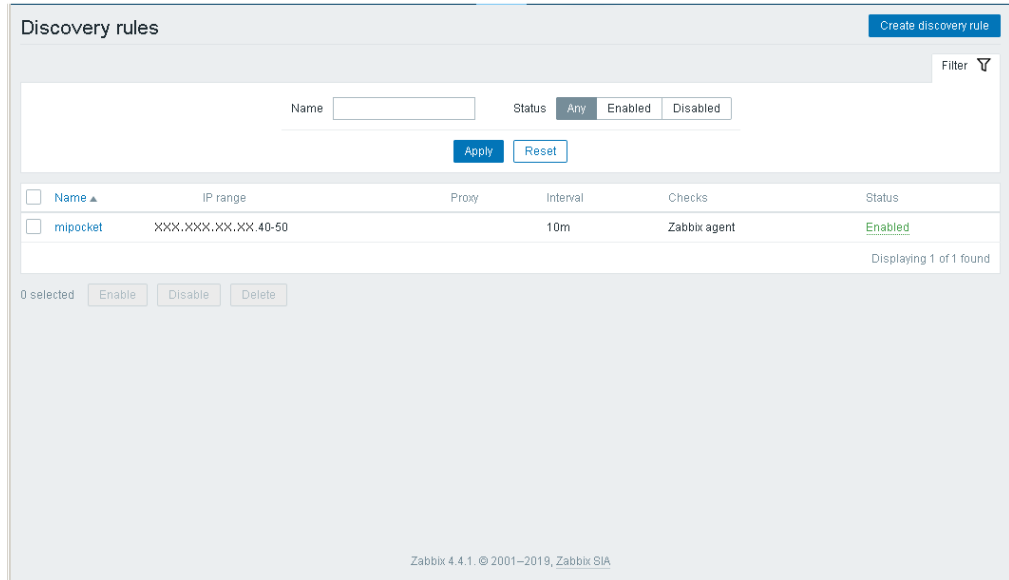
### 3.7.3. Displaying the logs

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.

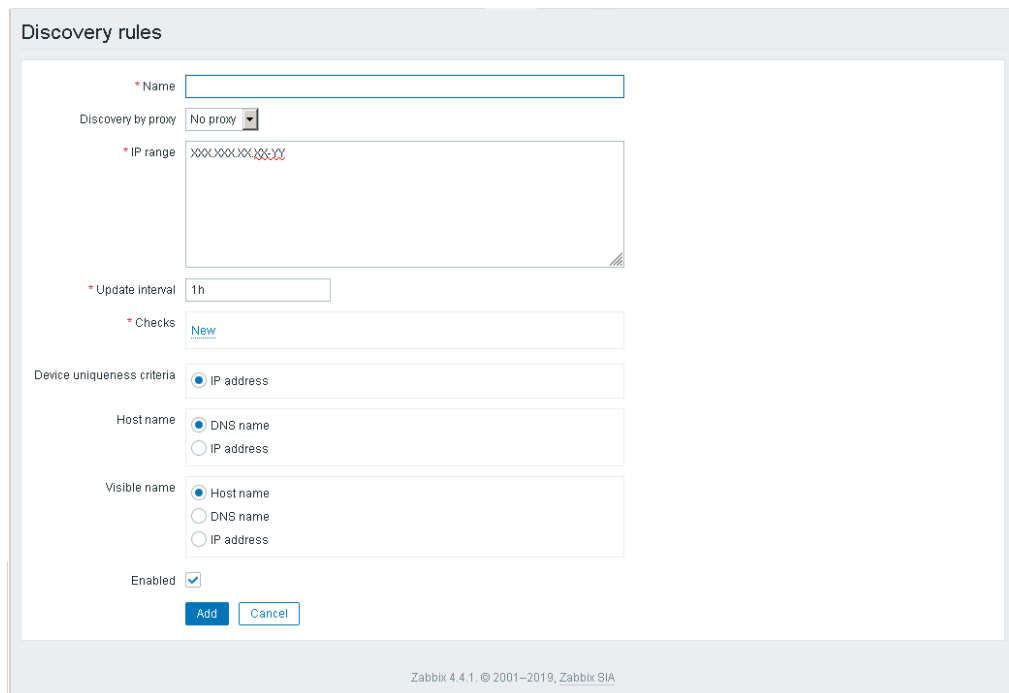
## 3.8. Configuring nmap

### 3.8.1. Creating a nmap discovery rule

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



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

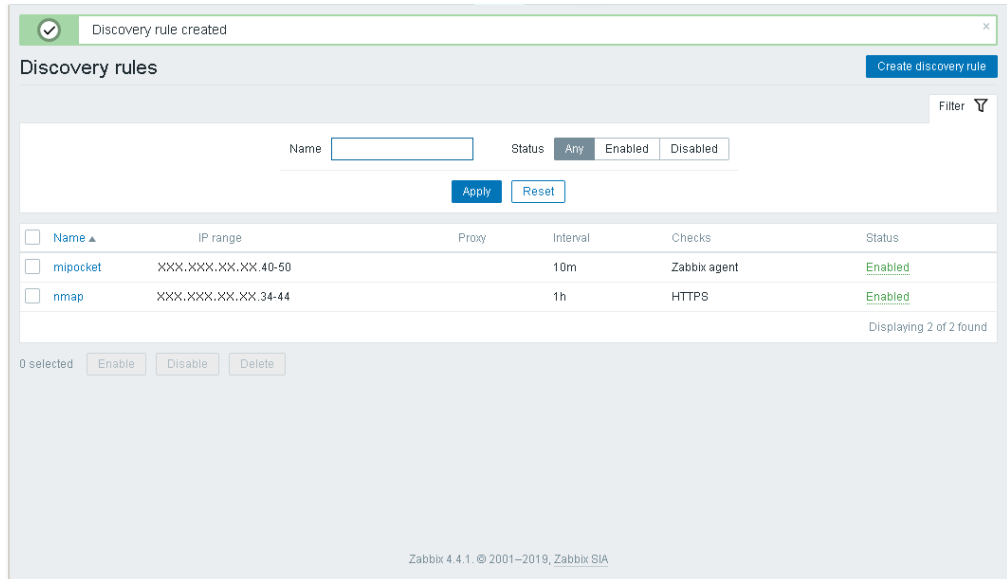


3. Complete the **Name** and **IP range** fields.
4. Configure the check type.

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

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

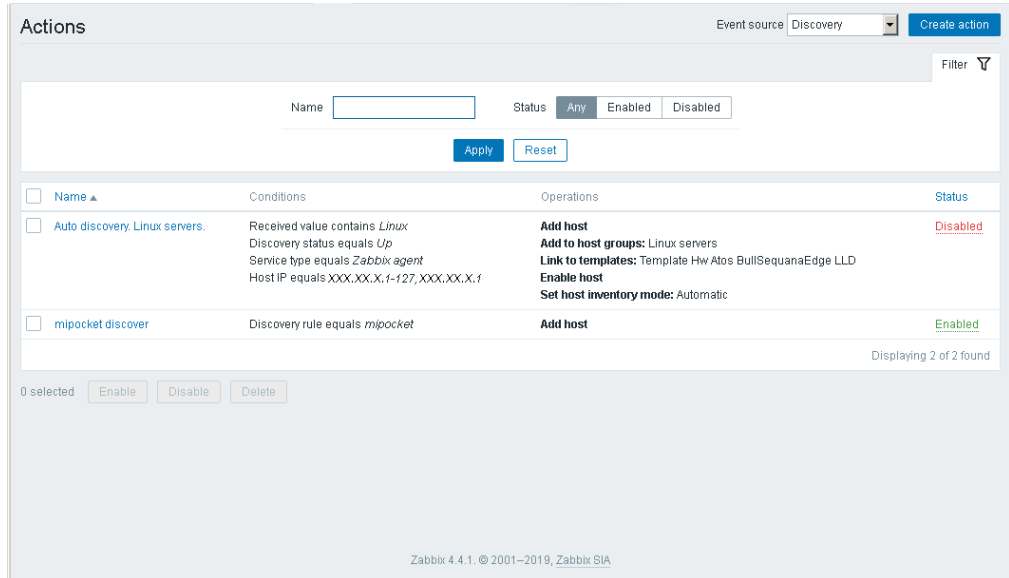
5. Save the discovery rule.  
Click **Add** to complete changes.  
The nmap discovery rule is created.



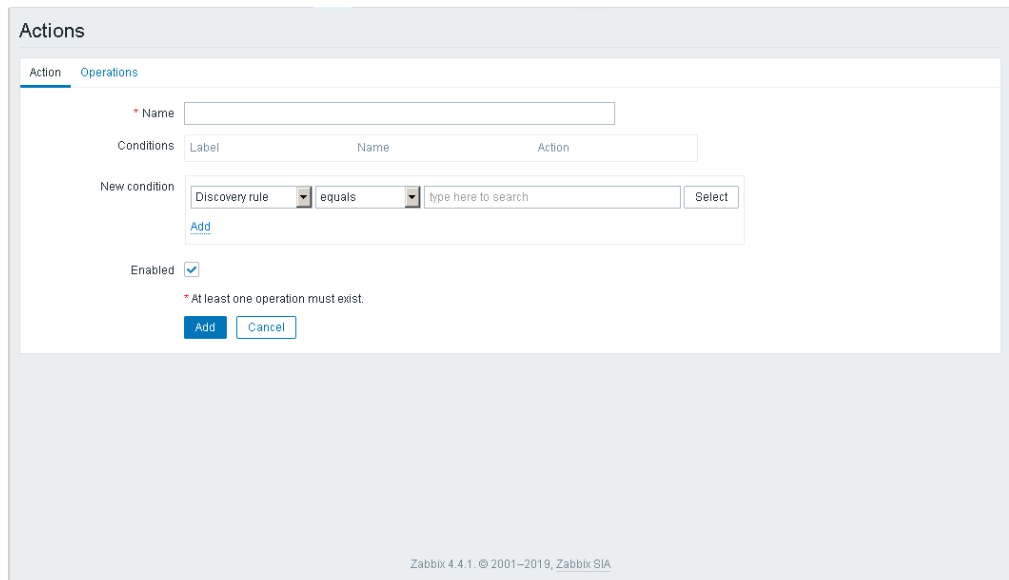
## 3.8.2. Creating a nmap action

### 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.



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, with the 'Operations' tab selected. The 'Default subject' field contains the text 'Discovery: {DISCOVERY.DEVICE.STATUS} {DISCOVERY.DEVICE.IPADDRESS}'. The 'Default message' field contains a template for a discovery rule, including placeholders for '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 message field, there is an 'Operations' section with a 'Details' tab selected and an 'Action' dropdown menu. A 'New' button is visible in the 'Action' dropdown. A red asterisk indicates a required field: '\* At least one operation must exist.' At the bottom of the 'Operations' section 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.

This screenshot shows the same 'Actions' configuration page as the previous one, but now the 'Add host' operation has been added to the 'Operations' list. The 'Action' dropdown menu now shows 'Add host' as the selected option, with 'Edit' and 'Remove' links next to it. The 'New' button is still present. The 'Add' and 'Cancel' buttons remain at the bottom. The footer text is identical to the previous screenshot: 'Zabbix 4.4.1. © 2001–2019, Zabbix SIA'.

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**.

Actions

Action Operations

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

Default message: Discovery rule: {DISCOVERYRULE.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  
 Add host Edit Remove

Operation details: Operation type: Add to host group  
 \* Host groups: type here to search Select  
 Add Cancel

\* At least one operation must exist.  
 Add Cancel

Zabbix 4.4.1. © 2001–2019, Zabbix SIA

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

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

Actions

Action Operations

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

Default message: Discovery rule: {DISCOVERYRULE.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  
 Add host Edit Remove  
 Add to host groups: Discovered hosts Edit Remove  
 New

\* 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.

The screenshot shows the Zabbix Actions configuration interface. At the top, a green notification bar says "Action added". Below it, the "Actions" section has a search bar and a "Create action" button. A filter dropdown is set to "Discovery". The main table lists three actions:

<input type="checkbox"/>	Name	Conditions	Operations	Status
<input type="checkbox"/>	Auto discovery: Linux servers.	Received value contains <i>Linux</i> Discovery status equals <i>Up</i> Service type equals <i>Zabbix agent</i> Host IP equals <i>XXX.XX.X.1-127,XXX.XX.X.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"/>	mpocket discover	Discovery rule equals <i>mpocket</i>	<b>Add host</b>	Enabled
<input type="checkbox"/>	nmap discovery	Discovery rule equals <i>nmap</i>	<b>Add host</b> <b>Add to host groups:</b> Discovered hosts	Enabled

At the bottom, it says "0 selected" with buttons for "Enable", "Disable", and "Delete". The footer indicates "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.

Media types

Create media type Import

Filter

Name  Status **Any** Enabled Disabled

Apply Reset

<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: "devttyS0"	Test

Displaying 2 of 2 found

0 selected Enable Disable Export Delete

Zabbix 4.4.1. © 2001–2019, Zabbix SIA

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

Media types

Media type Options

\* Name

Type **Email**

\* SMTP server

SMTP server port

\* SMTP helo

\* SMTP email

Connection security **None** STARTTLS SSL/TLS

Authentication **None** Username and password

Message format **HTML** Plain text

Description

Enabled

Add Cancel

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 'Media type' tab is active, and the 'Options' sub-tab is selected. 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:**

Buttons: Add, Cancel

Footer: 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 notification banner at the top says 'Media type added'. The page includes a search bar and a table of media types.

Buttons: Create media type, Import, Filter, Apply, Reset, Enable, Disable, Export, Delete

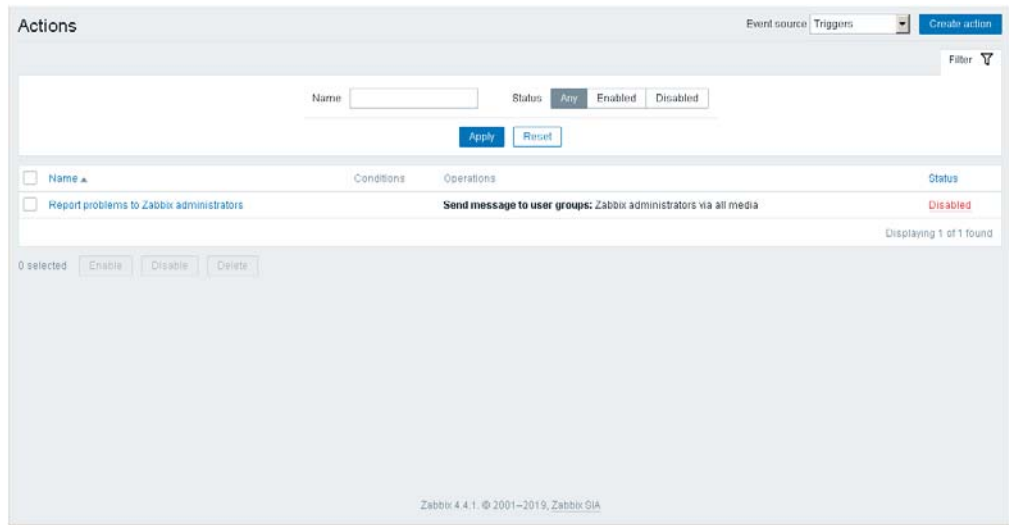
Name	Type	Status	Used in actions	Details	Action
Email	Email	Enabled		SMTP server: "mail.example.com", SMTP helo: "example.com", SMTP email: "zabbix@example.com"	Test
MyEmail	Email	Enabled		SMTP server: "XXX.XX.X.XX", SMTP helo: "atos.net", SMTP email: "XX.XX@atos.net"	Test
SMS	SMS	Enabled		GSM modem: "udevtyS0"	Test

Footer: Zabbix 4.4.1. © 2001–2019, Zabbix SIA

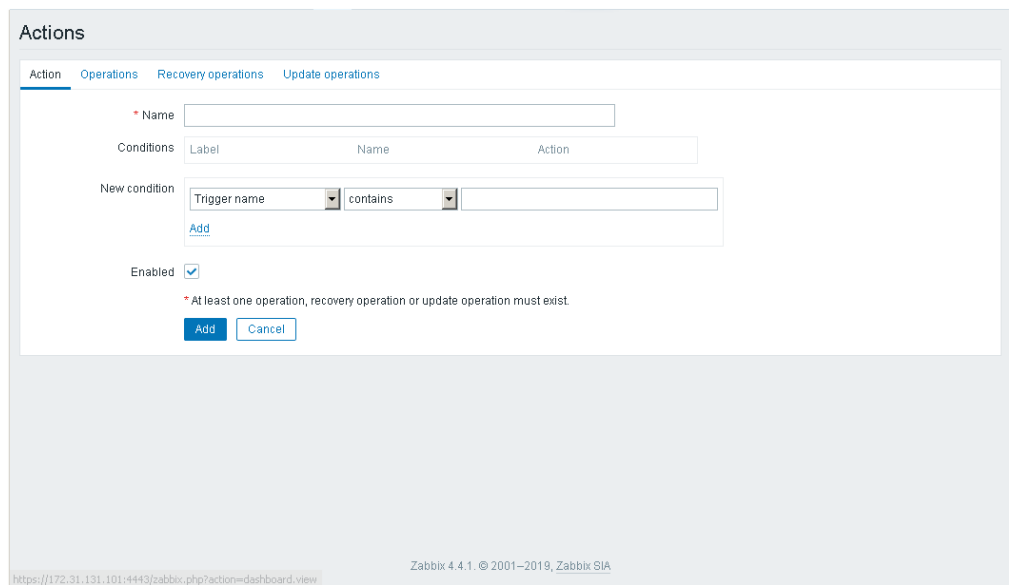
7. Click **Test** to send a test email.

### 3.9.2. Creating an action

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



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



4. Complete the **Name** field.

5. Click the **Operations** tab.

The screenshot shows the 'Actions' configuration page in Zabbix, with the 'Operations' tab selected. The page includes the following elements:

- Navigation tabs: 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 table with columns: Steps, Details, Start in, Duration, Action. A 'New' link is visible under the 'Steps' column.
- Validation message: \* At least one operation, recovery operation or update operation must exist.
- Buttons: Add, Cancel.
- Footer: Zabbix 4.4.1. © 2001–2019, Zabbix SIA

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

The screenshot shows the 'Actions' configuration page in Zabbix, with the 'Operations' tab selected. The 'New' operation configuration is visible, including the following elements:

- Navigation tabs: 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 table with columns: Steps, Details, Start in, Duration, Action.
- Operation details section:
  - Steps: 1 - 1 (0 - infinitely)
  - Step duration: 0 (0 - use action default)
  - Operation type: Send message
  - Validation 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
- Buttons: Add, Cancel.
- Validation message: \* At least one operation, recovery operation or update operation must exist.
- Footer: 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 interface. It includes tabs for 'Action', 'Operations', 'Recovery operations', and 'Update operations'. The 'Operations' tab is selected, displaying a table with one operation: 'Send message to users: Admin (Zabbix Administrator) via MyEmail'. The table has columns for 'Steps', 'Details', 'Start in', 'Duration', and 'Action'. Below the table, there are 'Add' and 'Cancel' buttons. The footer indicates 'Zabbix 4.4.1. © 2001–2019, Zabbix SIA'.

8. Save the action.
 

Click **Add** to complete changes.

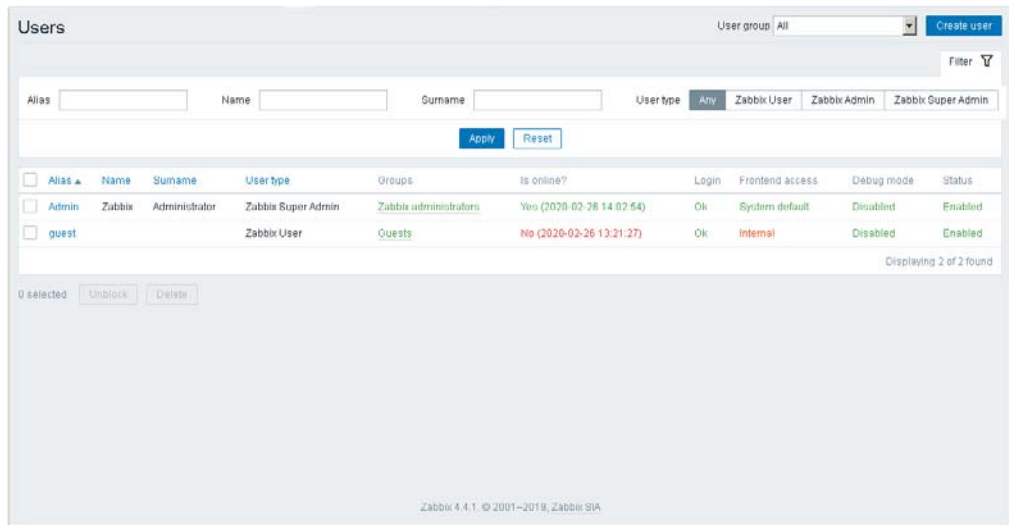
The action is created.

### Example

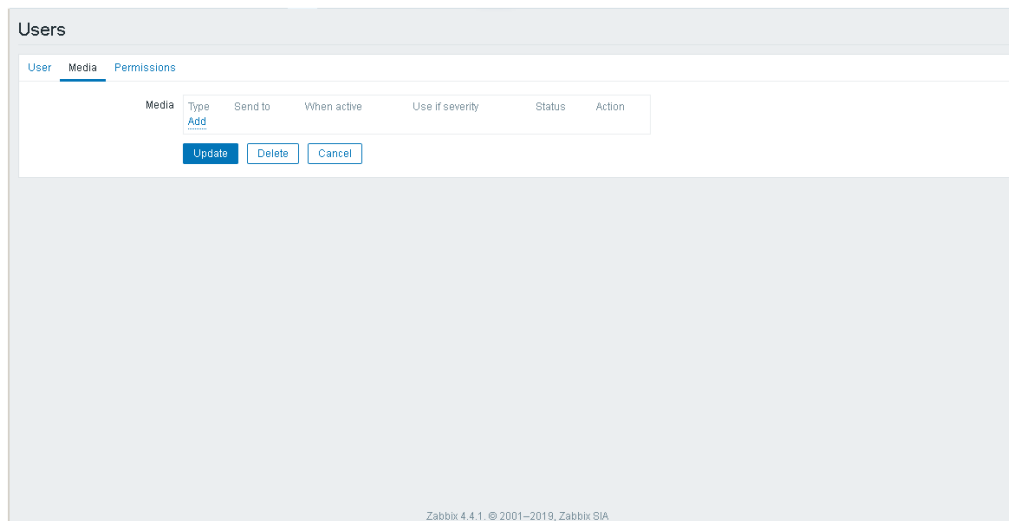
The screenshot shows the 'Actions' list page. At the top, there is a notification 'Action added'. The page has a search bar for 'Name' and a 'Status' filter with options 'Any', 'Enabled', and 'Disabled'. Below the search bar are 'Apply' and 'Reset' buttons. The main content is a table with columns for 'Name', 'Conditions', 'Operations', and 'Status'. Two actions are listed: 'Report problems to Zabbix administrators' (Status: Disabled) and 'Send message to users: Admin (Zabbix Administrator) via MyEmail' (Status: Enabled). At the bottom, there are '0 selected', 'Enable', 'Disable', and 'Delete' buttons. The footer indicates 'Zabbix 4.4.1. © 2001–2019, Zabbix SIA'.

### 3.9.3. Configuring the user

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

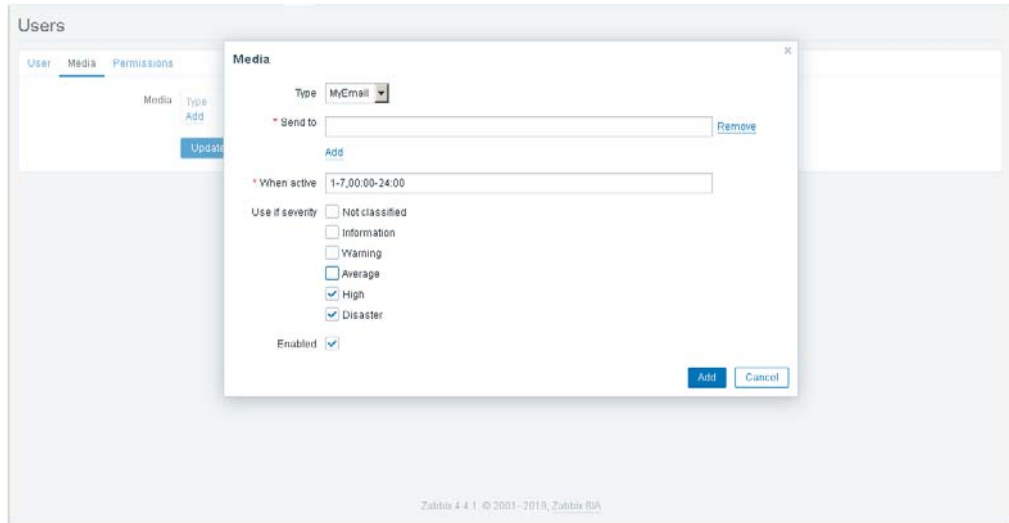


2. Select the user required. A new page opens.
3. Click the **Media** tab.



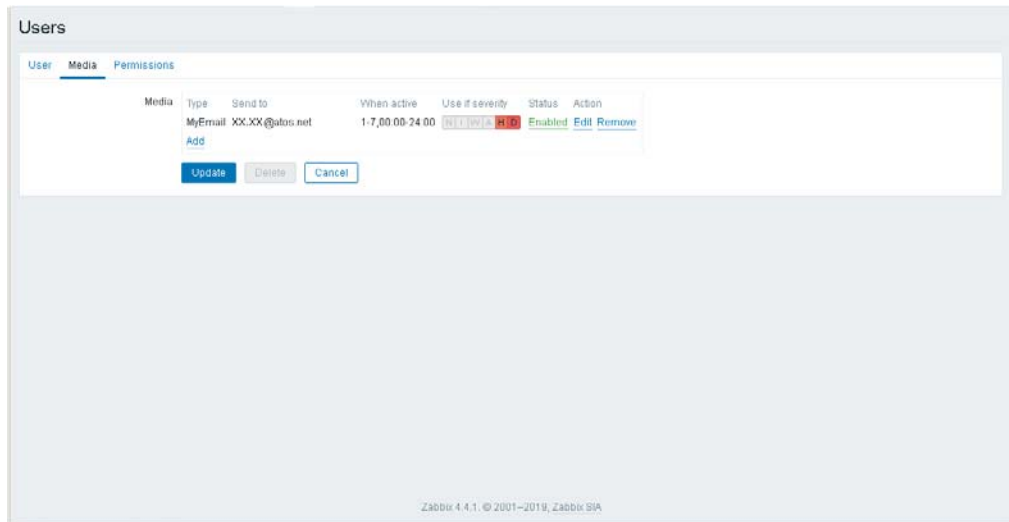
- In the **Media** section, click **Add**. The **Media** page opens.

### Example



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

### Example



- 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.

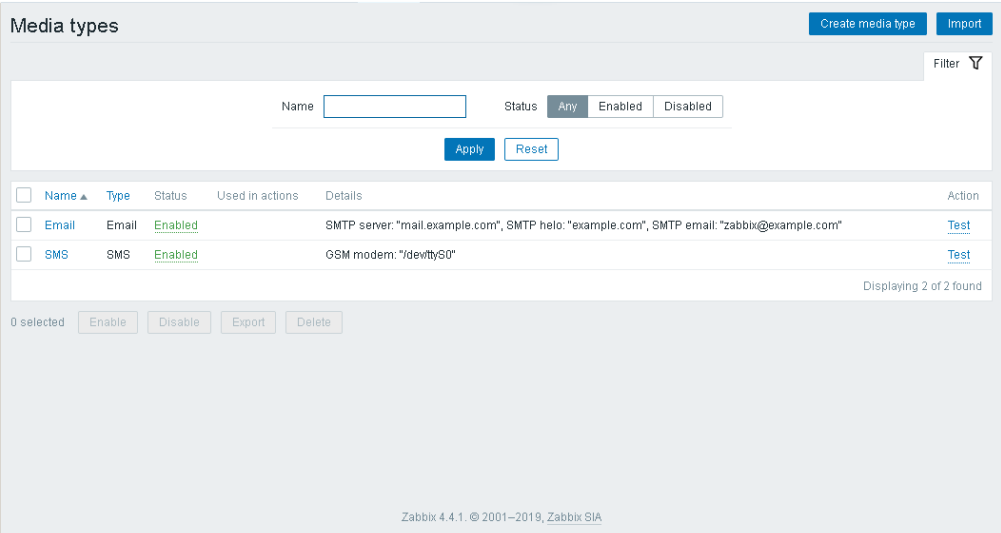
---

**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 web interface. 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 area contains a table with columns: Name, Type, Status, Used in actions, Details, and Action. Two media types are listed: 'Email' and 'SMS', both with a status of 'Enabled'. Below the table, there are buttons for 'Apply' and 'Reset'. At the bottom of the page, there is a footer with the text '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.

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

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

### Example

Media types

Create media type Import

Filter

Name  Status **Any** Enabled Disabled

Apply Reset

<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>
<input type="checkbox"/>	SMS France	Script	Enabled		Script name: "zabbix-smsmode"	<a href="#">Test</a>

Displaying 3 of 3 found

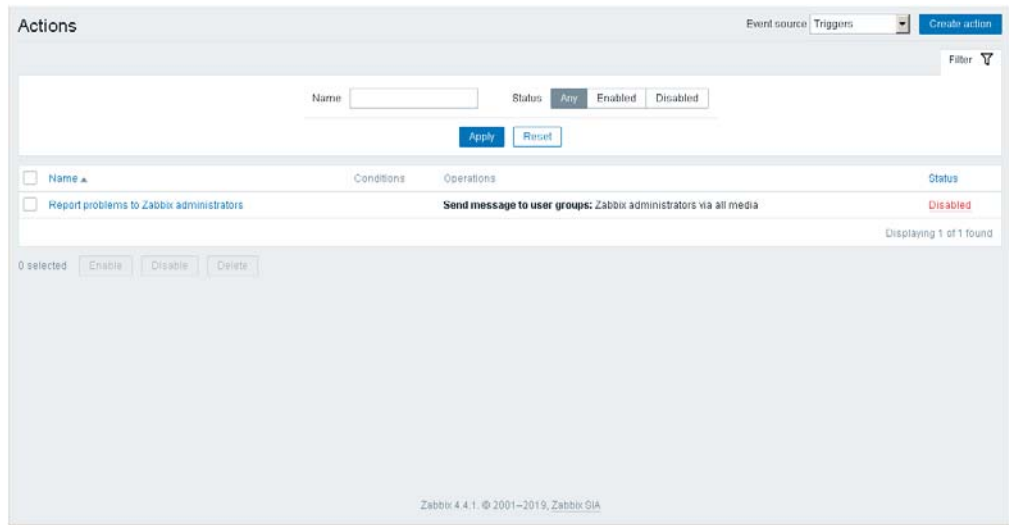
0 selected Enable Disable Export Delete

Zabbix 4.4.1. © 2001–2019, Zabbix SIA

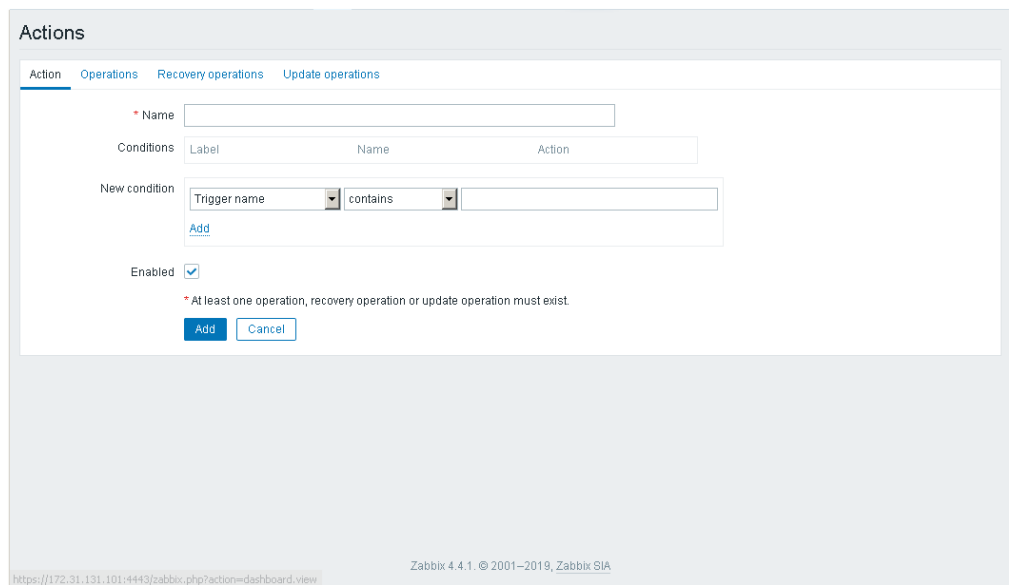
8. Click **Test** to send a test SMS.

### 3.10.2. Creating an action

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



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



4. Complete the **Name** field.

5. Click the **Operations** tab.

The screenshot shows the 'Actions' configuration page in Zabbix, with the 'Operations' tab selected. The page includes the following elements:

- Navigation tabs: Action, **Operations**, Recovery operations, Update operations.
- Default operation step duration: 1h (input field).
- Default subject: Problem: {EVENT.NAME} (input field).
- 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} (text area).
- Pause operations for suppressed problems: .
- Operations table with columns: Steps, Details, Start in, Duration, Action. A 'New' link is visible under the 'Steps' column.
- Validation message: \* At least one operation, recovery operation or update operation must exist.
- Buttons: Add, Cancel.
- Footer: Zabbix 4.4.1. © 2001–2019, Zabbix SIA.

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

The screenshot shows the 'Actions' configuration page in Zabbix, with the 'Operations' tab selected. The 'New' operation configuration is visible, including the following elements:

- Navigation tabs: Action, **Operations**, Recovery operations, Update operations.
- Default operation step duration: 1h (input field).
- Default subject: Problem: {EVENT.NAME} (input field).
- 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} (text area).
- Pause operations for suppressed problems: .
- Operations table with columns: Steps, Details, Start in, Duration, Action.
- Operation details section:
  - Steps: 1 - 1 (0 - infinitely)
  - Step duration: 0 (0 - use action default)
  - Operation type: Send message (dropdown menu)
  - Validation message: \* At least one user or user group must be selected.
  - Send to User groups: User group (input field), Action (button), Add (link).
  - Send to Users: User (input field), Action (button), Add (link).
  - Send only to: - All - (dropdown menu)
  - Default message: .
  - Conditions: Label (input field), Name (input field), Action (button), New (link).
- Buttons: Add, Cancel.
- Footer: 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 interface. The 'Operations' tab is selected, displaying a table with one operation: 'Send message to users: Admin (Zabbix Administrator) via SMS France'. The 'Default message' field contains a template with variables like {EVENT.TIME}, {EVENT.DATE}, {EVENT.NAME}, {HOST.NAME}, {EVENT.SEVERITY}, and {EVENT.ID}. The 'Pause operations for suppressed problems' checkbox is checked. At the bottom, there are 'Add' and 'Cancel' buttons.

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

### Example

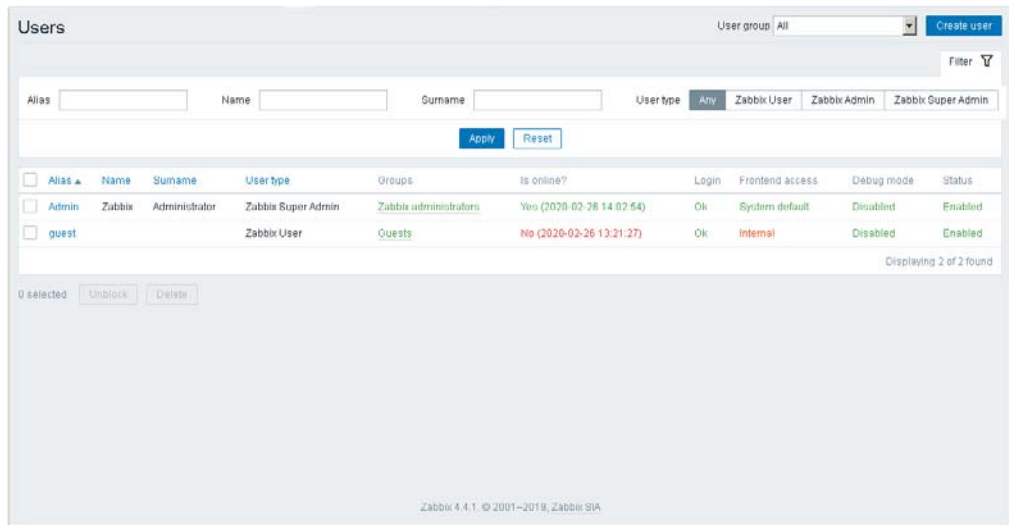
The screenshot shows the 'Actions' list page. A notification 'Action added' is displayed at the top. The table lists three actions:

Name	Conditions	Operations	Status
Report problems to Zabbix administrators		Send message to user groups: Zabbix administrators via all media	Disabled
testIPB		Send message to users: Admin (Zabbix Administrator) via SMS France	Enabled

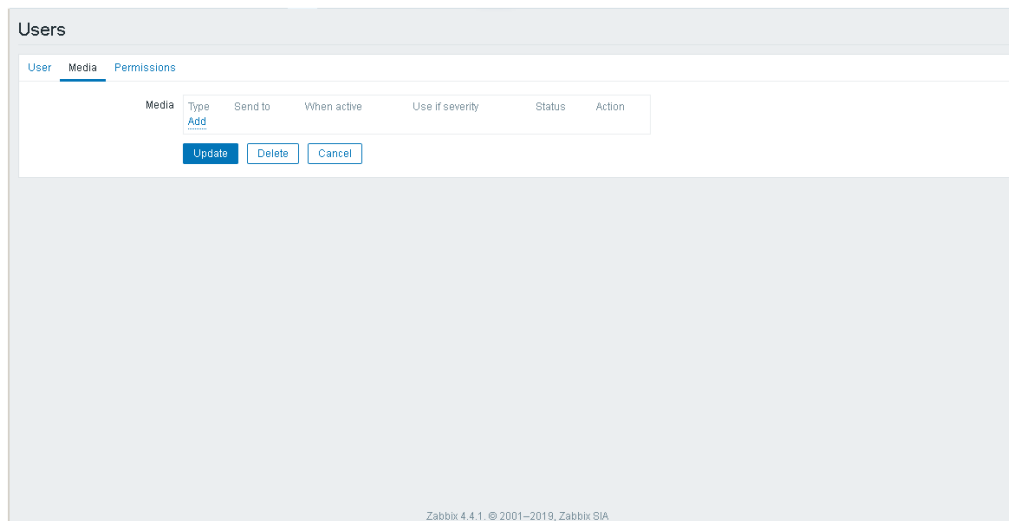
The 'Enabled' status of the last action is highlighted in green. At the bottom, there are 'Enable', 'Disable', and 'Delete' buttons for the selected row.

### 3.10.3. Configuring the user

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

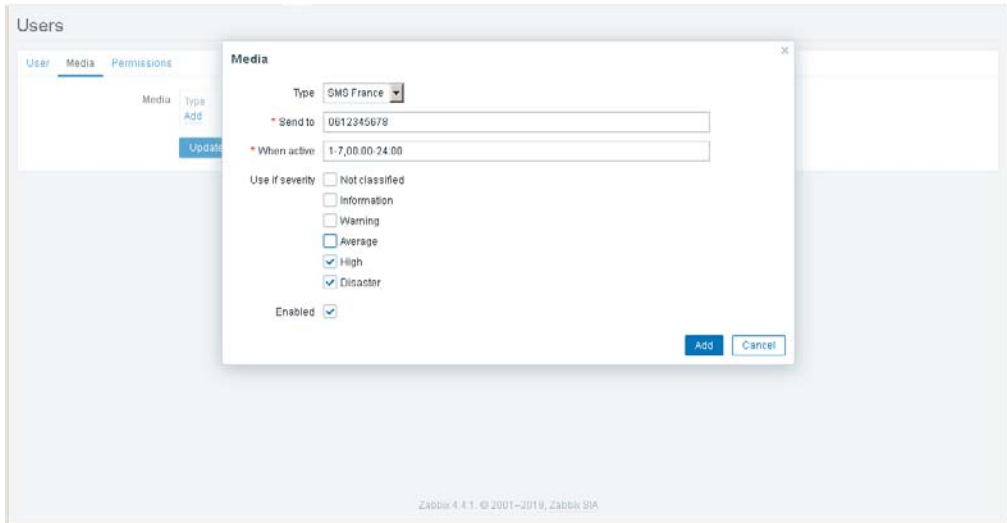


2. Select the user required. A new page opens.
3. Click the **Media** tab.



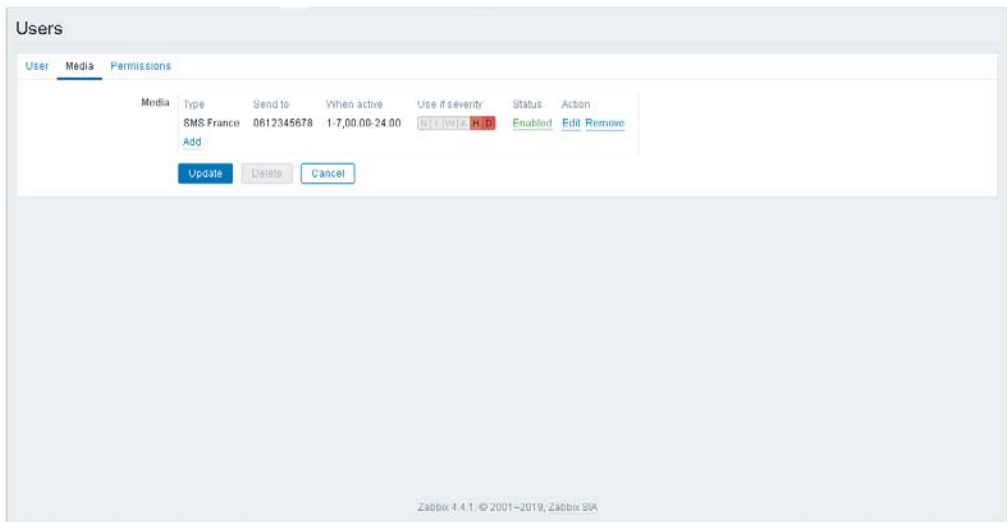
4. In the **Media** section, click **Add**. The **Media** page opens.

### Example



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

### Example



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**