



Visualization



om:

<https://pandorafms.com/manual/!775/>

permanent link:

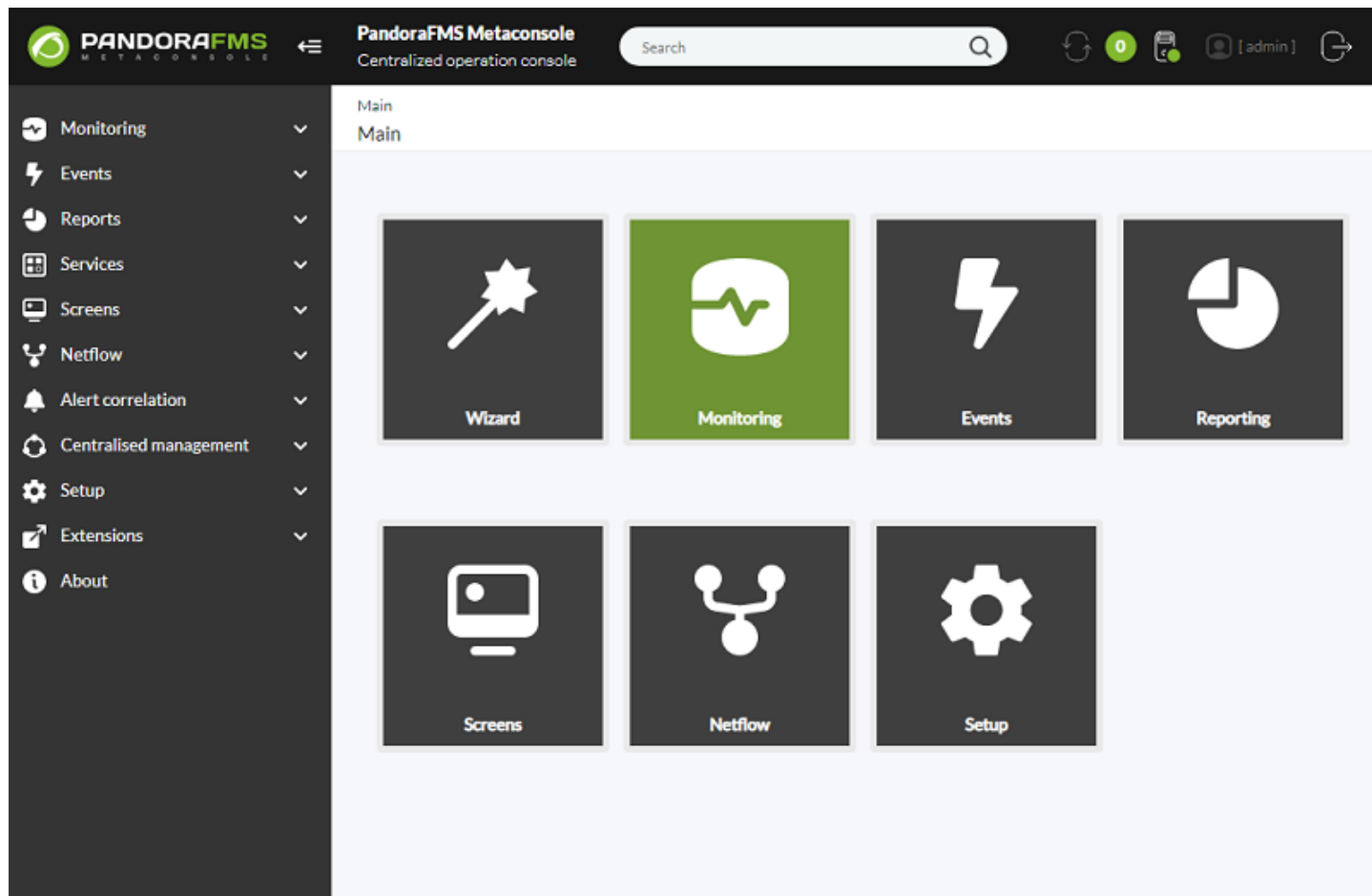
https://pandorafms.com/manual/!775/en/documentation/pandorafms/command_center/05_visualization

2024/03/18 21:03



Visualization

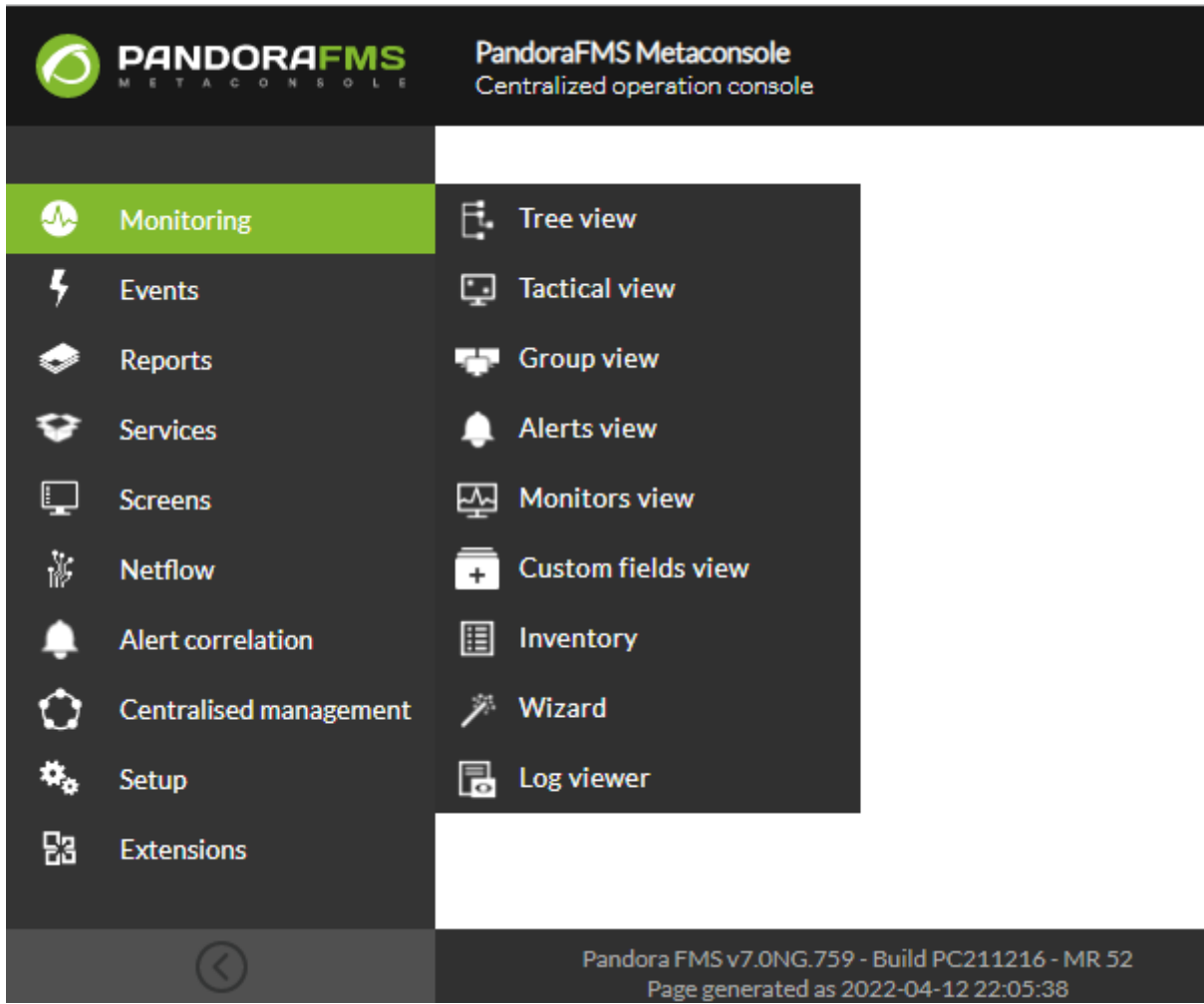
E This section will explain the Metaconsole options that refer to the navigation/display of the agent data, and the Instance modules and alerts from the Metaconsole.



Monitoring

E Data can be displayed in the following ways:

- Tree view.
- Tactical view.
- Group view.
- Alerts view.
- Monitors view.
- Custom fields view.
- Inventory.
- Wizard.
- Log viewer.



Tree View

PandoraFMS Metaconsole
Centralized operation console

Search

6 (admin)

Tree view Tactical view Group view Alerts view Monitors view Custom fields view Inventory Wizard Log viewer

Show Options

Groups found: 12

- Applications [21:1:6:9:6]
- Databases [1:1]
- Firewalls [2:1:1]
- Network [33:3:2:28]
- Servers [1174:1:193:54:552:375]
- Unknown [4:1:2:1]
- Web [2:2]
- Workstations [17:16:1]

Pandora FMS v7.0NG.759 - Build PC211216 - MR 52
Page generated as 2022-04-12 22:37:44

This view allows agent monitors to be displayed in a tree view. You can have access through Monitoring → Tree view.

It is possible to filter by module status (Critical, Normal, Warning and Unknown) and search by agent name or by group. In addition, it is also possible to have the uninitiated agents or modules displayed (Show not init modules and Show not init agents options), as well as the complete hierarchy.

In each level, the counting of the number of items of its branch is shown: total number of elements, Critical (red color), Warning (yellow color), Unknown (gray color), not uninitiated modules (blue) and normal status (green color).

The first level is loaded first. By clicking on the items of each level, the branch with the items it contains will be displayed.

This is a group tree where the agents are displayed, filtered by the group they belong to.

✓ Show Options

Search group

Search agent

Show not init modules

Show not init agents

Show full hierarchy

Agent status All ▼

Filter 🔍

🔄 Groups found: 12

- + 📁 Applications [21:1:6:9:6]
 - + ■ 000 Agent for automated testing [4:1:1:3]
 - + ■ 000 Agent for automated testing [1:1]
 - + ■ 001 Agent for services testing [1:1]
 - + ■ 001 Agent for services testing [1:1]

Items shown in the group are restricted by the ACLs permissions and by the the permissions for Tags that the user has

Levels

Groups

This is the first level.

Displaying the branch of one Group, it shows the agents contained in that Group.

The counting next to the group name refers to the number of agents it contains that are in each status.

Only the enabled agents that have at least one module enabled and initiated will be shown.

> Show Options

Groups found: 12

- + Applications [21:1:6:9:6]
- + Databases [1:1]
- + Firewalls [2:1:1]
- + Network [33:3:2:28]
- + Servers [1174:1:193:54:552:375]
- + Unknown [4:1:2:1]
- + Web [2:2]
- + Workstations [17:16:1]

Agents

If you display the branch of one Agent, the modules that this agent contains will be shown.

The counting next to the name of the Agent refers to the number of Modules it contains that are in each status.

Groups found: 12

- + Applications [21:1:6:9:6]
 - + 000 Agent for automated testing [4:1:1:3]
 - + 000 Agent for automated testing [1:1]
 - + 001 Agent for services testing [1:1]
 - + 001 Agent for services testing [1:1]
 - + MetaManu [9:4:5]
 - + stod.100 [11:1:10]
 - + test2stod [7:7]
 - + test_isma [10:10]
 - + test_snmp_stod [4:1:2:1]
- + Databases [1:1]

By clicking on the agent name, it will show information about it at the right: Name, IP address, date of last update, operative system and also an event graph and another one showing the accesses of the last 24 hours.

In order for the data related to agent *Custom Fields* to be displayed in this Metaconsole information window, activate in nodes the Display up front token explained [in this section](#).

✕

✓ **Agent data**

Agent name	KOLDO_AGENT
IP Address	192.168.80.34 ⓘ
Interval	5 minutes
Description	Created by koldo
Last contact / Remote	27 minutes 31 seconds / September 15, 2021, 12:15 pm
Next agent contact	<div style="background-color: #76b82a; color: white; padding: 2px 5px; display: inline-block;">100%</div>

[Go to agent edition](#) ✎

✓ **Advanced information**

Agent version	7.0NG.760(Build 200504)
Agent Extra Info ⓘ	California 527, 3rd Floor, Rack1

✓ **Agent access rate (24h)**

Time	Access Rate
12:09	3
13:09	12
14:09	12
15:09	12
16:09	12
17:09	12
18:09	12
19:09	12
20:09	12
21:09	12
22:09	12
23:09	12
00:09	12
01:09	12
02:09	12
03:09	12
04:09	12
05:09	12
06:09	12
07:09	12
08:09	4

✓ **Events (24h)**

Date/Time	Event Type
14 Sep 12:43	Error
14 Sep 16:43	Event
14 Sep 20:43	Error
15 Sep 00:43	Event
15 Sep 04:43	Error
15 Sep 08:43	Event
15 Sep 12:43	Event

Modules

The module is the last branch of the tree.

The screenshot shows the Pandora FMS interface. On the left, a tree view under 'test_isma [10:10]' lists various modules. The 'Windows version' module is selected. On the right, a pop-up window displays the configuration for the 'WINDOWS VERSION' module.

Property	Value
Name	WINDOWS VERSION
Interval	5 minutes
Warning status	Str.:
Critical status	Str.:
Module group	General
Description	Operating system version
Last status change	5 days
Last data	Microsoft Windows Server 2016 Standard

At the bottom of the pop-up window, there is a button labeled 'Go to module edition' with a pencil icon.

By clicking on the module name, it will show information about it at the right. Next to the name of each module, in this branch several buttons will appear:

- **Module Graph:** A *pop-up* will appear with the module graph.
- If the module contains alerts, it will show an alert icon. By clicking on the icon, it will show information about module alerts at the right side: The templates they belong to and their actions.
- If the module has a magnifying glass icon, it indicates that the text for last data is very long and you will have to click on it to view its entire contents.
- **Information *In Raw state* :** You can have access to the module view where the received data are shown in one table.

Module: Total Virtual Memory Size

Choose a time from now 3 years

Specify time range

Timestamp from: 2022/4/12 18:7

Timestamp to: 2022/4/12 18:7

Total items: 7

Data	Time
10,864,936	12 April 2022 06:28:59 PM
10,864,936	11 April 2022 06:28:55 PM
10,864,936	10 April 2022 06:24:01 PM
10,864,936	09 April 2022 06:22:07 PM
10,864,936	08 April 2022 06:20:51 PM

Tactical View

The tactical view of the Metaconsole is made of:

- A table with a summary of the agents and module status.
- A table with the last events.
- A table with the last activity of the instances of Pandora FMS.

PandoraFMS Metaconsole
Centralized operation console

Search

Tree view **Tactical view** Group view Alerts view Monitors view Custom fields view Inventory Wizard Log viewer

Report of status

Agents by status

	219		41
	410		17
	567		

Monitors by status

	278		54
	5522		170
	39		

Triggered alerts

2

Node overview

2

Report of events (1 hours)

Important events by severity

0	0	0	0
---	---	---	---

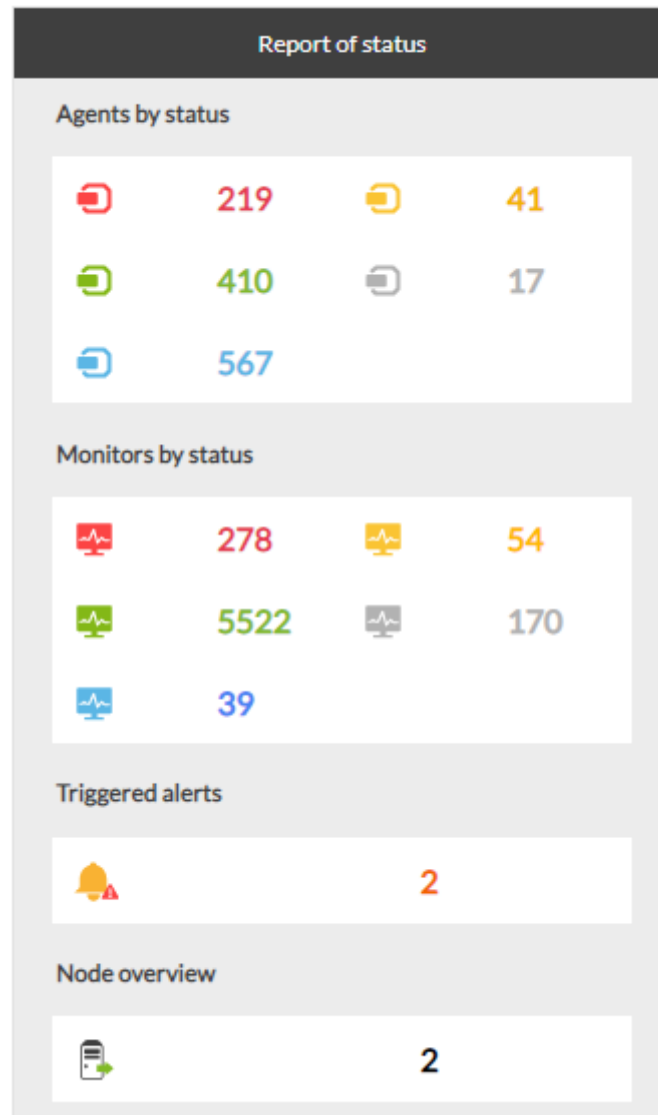
Info of status in events (1 hours)

Last activity in Pandora FMS console

User	Action	Date	Source IP	Comments
admin	User management	2 h	192.168.80.1	Updated user Documentation
admin	User management	2 h	192.168.80.1	Created user Documentation
admin	User management	2 h	192.168.80.1	Added profile for user
admin	Logoff	9 h	192.168.80.1	Logged out
admin	Metaconsole node	9 h	:::1	Node koldo_server modified

Pandora FMS v7.0NG.759 - Build PC211216 - MR 52
Page generated as 2022-04-13 00:29:49

Information about Agents and Modules



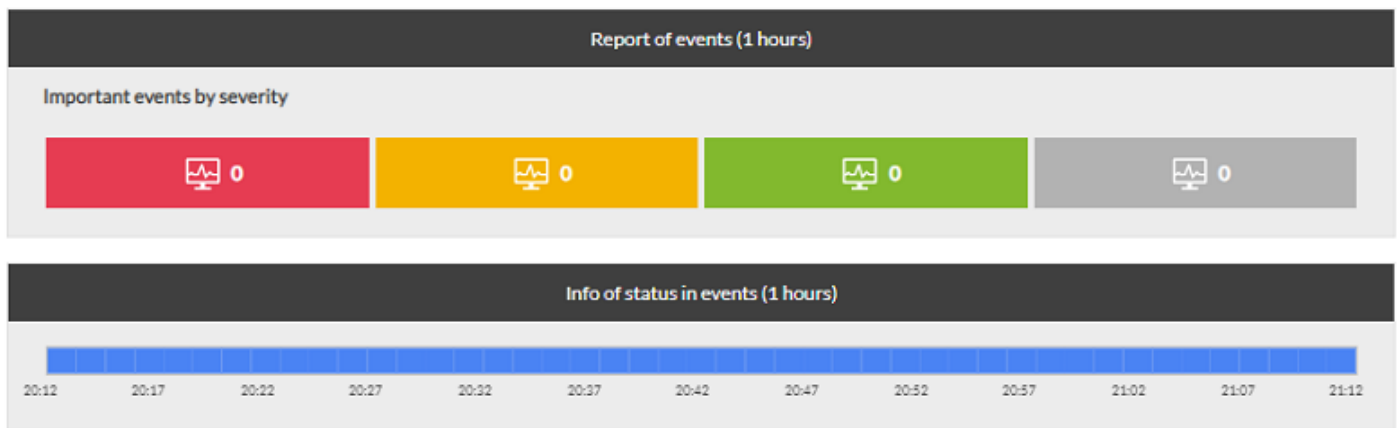
The status report is displayed in a summary table:

- Agents by status.
- Monitors by status.
- Triggered alerts.
- Node summary.

Except for the node summary, you can click on each numerical value to get more information on each topic.

Last Events

On the one hand, a table with the events of the last hour summed up in their different status is shown (Critical, Warning, Normal y Unknown). On the other hand, the same events of the last hour are shown according to their order of arrival to the Metaconsole (info of status in events).



This view only has briefing purposes, the events cannot be validated and their information cannot be displayed in detail.

Group View

The group view is a table with the groups of each Instance and the following information about each one:

- Group name. In the first place is the All group, if secondary groups are being used it will have an informative icon.
- Agent total number.
- Group status (the worst status from their agents).
- Number of agents in Unknown status.
- Number of agents in No init status.
- Number of agents in Critical status.
- Number of modules in Unknown status.
- Number of modules in No init status.
- Number of modules in Normal status.
- Number of modules in Warning status.
- Number of modules in Critical status.
- Number of alerts fired.

Monitoring / Views

GROUP VIEW

Summary of the status groups

Agents

Modules

8.24%

1.43%

85.30%

3.94%

1.00%

1.02%

0.15%

89.97%

8.80%

0.06%

Total items: 11

		Agents						Modules					
Force	Group/Tags	Total	Unknown	Not initialised	Normal	Warning	Critical	Unknown	Not initialised	Normal	Warning	Critical	Alert triggered
<input checked="" type="radio"/>	All	279	11	3	238	4	23	285	2	2915	5	33	1
<input type="radio"/>	Applications	5			2		3	2		77		4	
<input type="radio"/>	Databases	1			1					11			
<input type="radio"/>	Firewalls	1					1					1	
<input type="radio"/>	Network	3		2	1					1			
<input type="radio"/>	Servers	261	9		232	4	16	256		2729	4	25	
<input type="radio"/>	Unknown	2	1				1	14		74		1	1
<input type="radio"/>	Web	1					1	5		1		1	
<input type="radio"/>	Workstations	2	1		1			8	1	1			

Alert view

Alert view is a summary table with the alert information on the instances where the agent they belong to is displayed, as well as their module, used template, used action and the last time it was triggered.

PandoraFMS Metaconsole
Centralized operation console

Search

0

[admin]

Monitoring / Views
Alert details

> Filters

Policy	Standby Operations Agent	Module	Template	Action	Last triggered	Status
	nodo-1-pandorafms agent	Load Average	Warning condition	Mail to Admin (Default)	Unknown	

20

CSV

Monitor View


The monitor view is a table with information about the Instance monitors.

The modules that are shown are restricted by the ACL permissions and by the permissions by Tags that the user may have.



It could be filtered by:

- Group.
- Module status.
- Module group.
- Module name.
- Tags.
- Free search.
- Type of server.
- Type of data.


All monitors or just active monitors or deactivated monitors can be shown.

 Show Options

Group: Monitor status: Module group:


















Module name:  Search: Tags: 

Server type: Show monitors: Data type:

 Advanced options

Total items: 100

 0 1 2 3 4

Agent	Data type	Module name	Server type	Interval	Status	Graph	Warn	Data	Timestamp
1	DATA	Connections opened		5 minutes		 101	0/400 - 0/450	243 conns	Now
1	DATA	Dropped Bit...nothing		5 minutes		 101	N/A - N/A	349,416,065[...].jns 	Now
1	DATA	Network Tra...coming)		5 minutes		 101	N/A - 0/900K	213,017 [...].sec 	Now
1	DATA	Network Tra...going)		5 minutes		 101	N/A - 0/900K	658,153 [...].sec 	Now
1	PRDC	Server Status A		5 minutes		 101	N/A - N/A	37	Now
1	PRDC	Server Status B		5 minutes		 101	N/A - N/A	27	Now
1	PRDC	Server Status C		5 minutes		 101	N/A - N/A	0	Now

In this view, not all instance modules are shown, because it would not be feasible if they were big environments. A configurable number of modules is retrieved from each instance, 100 by default. This parameter is *Metaconsole Items* from the Visual Styles Administration Section, which can be modified, taking into account that if the number is very high, it may compromise the performance of the Metaconsole.

Custom Fields View

This view shows in a simple way the status of the agents according to their custom fields.

The Custom Fields view consists of:

- Search form.
- Custom filter management.
- Agent and module counting for each value of the selected custom field.
- General agent and module counting.
- List of agents filtered by the research.

Antenna

Agents by status: 121

97 24 0 0 0

Monitors by status: 2192

108 33 2051 0 0

Central

Agents by status: 132

102 30 0 0 0

Monitors by status: 2396

115 37 2244 0 0

Total counters

Total Agents

940 309 0 0 0

Total Modules

1,069 403 21,128 0 0

Show 15 items per page Search: Previous 1 2 3 4 5 84 Next

dispositivo	Agent	I.P	Server	Status
Tablet	stress_garrosh_596	127.0.0.1	garrosh	Critical
Tablet	stress_garrosh_175	127.0.0.1	garrosh	Critical
Tablet	stress_varian_1215	127.0.0.1	varian	Critical
Tablet	stress_varian_77	127.0.0.1	varian	Critical

Search Form:

- Group: This enables filtering by a specific group.
- Custom fields: It is mandatory to select an agent custom field. In order to select that field, it must have been previously created with the *Display up front* option checked in node in the following [section](#).
- Custom fields data: Value/s of the custom field.
- Status agents: State(s) of the agent.
- Module search: Module name.
- Status module: State(s) of module.

✓ Show Options

Group: All

Recursion:

Custom Fields: PandoraFMS

Module search:

Custom Fields Data:

- All
- [uri=PandoraFMS.com]Web PandoraFMS[/uri]
- [uri=www.pandorafms.com]ENLACE[/uri]
- [uri]PandoraFMS.com[/uri]

Status agents:

- All
- Critical
- Normal
- Not initialised
- Not normal
- Unknown
- Warning

Status module:

- All
- Critical
- Normal
- Not initialised
- Not normal
- Unknown
- Warning

Show

Export to CSV

Custom Filter Management:

- Create, update and delete filters: To improve access to the custom field view you can create, save and remove search filters. Choose the search parameters and click on the floppy disk icon to do it. A modal window will appear:
 - New Filter: Used for creating new filters. A name that has not been used before must be entered.

The screenshot shows a dialog box titled "Save filter" with a close button (X) in the top right corner. Below the title bar, there are two tabs: "New Filter" (active, highlighted in blue) and "Existing Filter". The "New Filter" tab contains a form with two input fields: "Filter name" (an empty text box) and "Group" (a dropdown menu with "All" selected). To the right of these fields is a dark button labeled "Create new filter" with a green circular refresh icon.

- Existing Filter: It is used for updating and deleting filters.




The screenshot shows the same "Save filter" dialog box, but the "Existing Filter" tab is active and highlighted in blue. The form fields are now: "Filter name" (a dropdown menu with "None" selected) and "Group" (a dropdown menu with "All" selected). To the right of these fields are two dark buttons: "Delete filter" and "Update filter", both with green circular refresh icons.

This filter management section will only be visible to administrator users..


- Load filters: Click on the arrow icon and select the desired filter.

The screenshot shows a dialog box titled "Load filter" with a close button (X) in the top right corner. Below the title bar, there is a form with one input field: "Filter name" (a dropdown menu with "filter-1" selected). To the right of this field is a dark button labeled "Load filter" with a green circular refresh icon.

- Add filters to a specific user: Assigning filters to users will be done in the user create/edit view. When users access this view, they will do so with the selected filter loaded.

Create user



User ID:

Administrator user

Extra info

Login error (i)

Local user (i)

Session time (i)

Language

Timezone (i)

Metaconsole access

Search custom field view (i)

Home screen (i)

Enable agent management

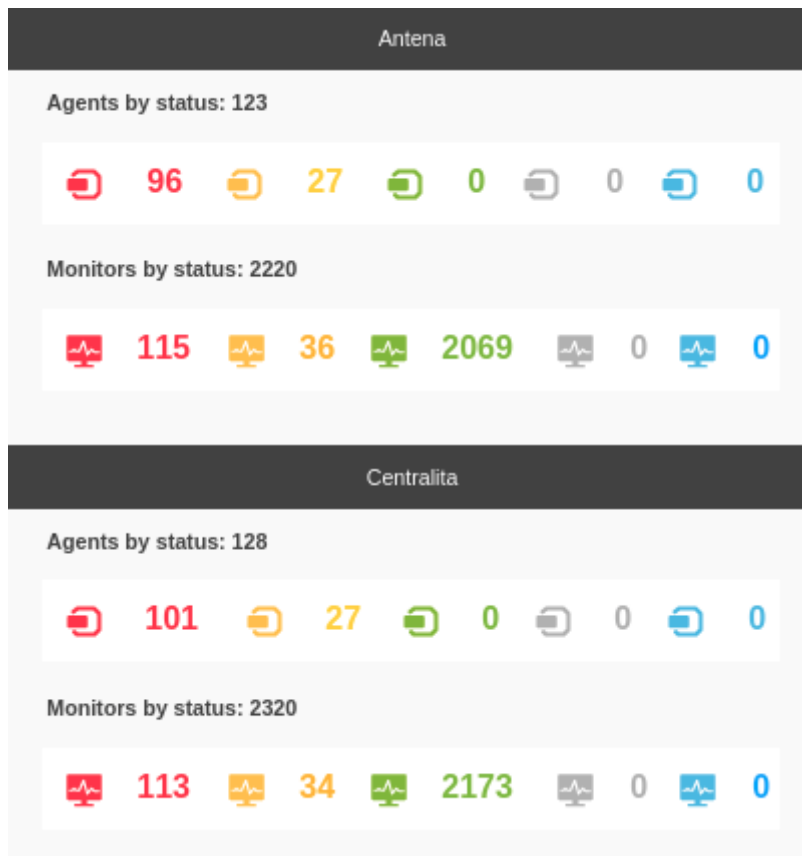
Enable node access (i)

Default event filter

Comments

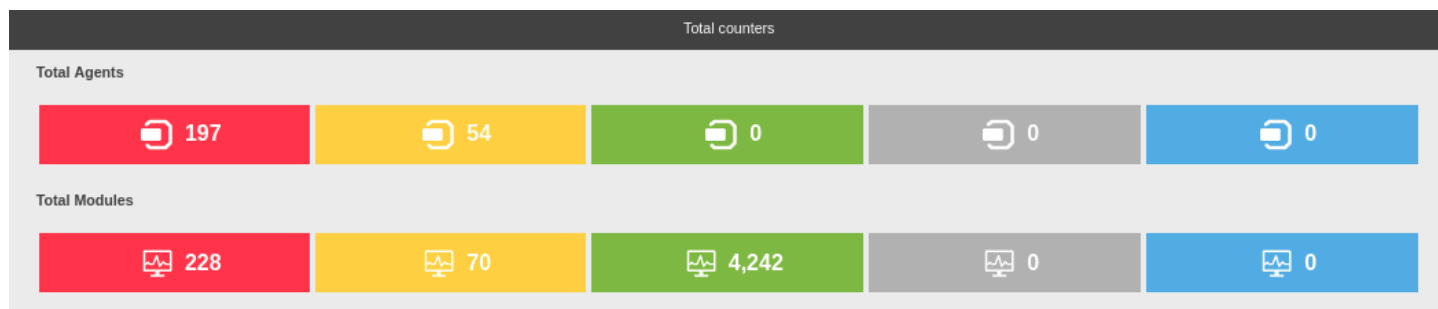
Agent and module counting for each value of the selected custom field:

In this view section, agent and module counting for each data of the selected custom field will be displayed in a simple way.



General agent and module counting:

This view section displays agent and module counting of all data of the custom fields.



List of agents:

It shows a list with the following agent information:

- Drop-down list where the following agent data will be shown with the selected custom field:
 - Module name.
 - Last data.
 - Threshold.
 - Interval time.
 - Last contact time.
 - Module status.
- Custom field value.
- Agent name.
- IP address.

- Server.
- Status.

This table is paged and can searches can be performed and sorted out by fields:

- Custom Field.
- Agent.
- IP address.
- Server.

dispositive	Agent	I.P	Server	Status
Central	stress_garosh_263	127.0.0.1	garosh	■

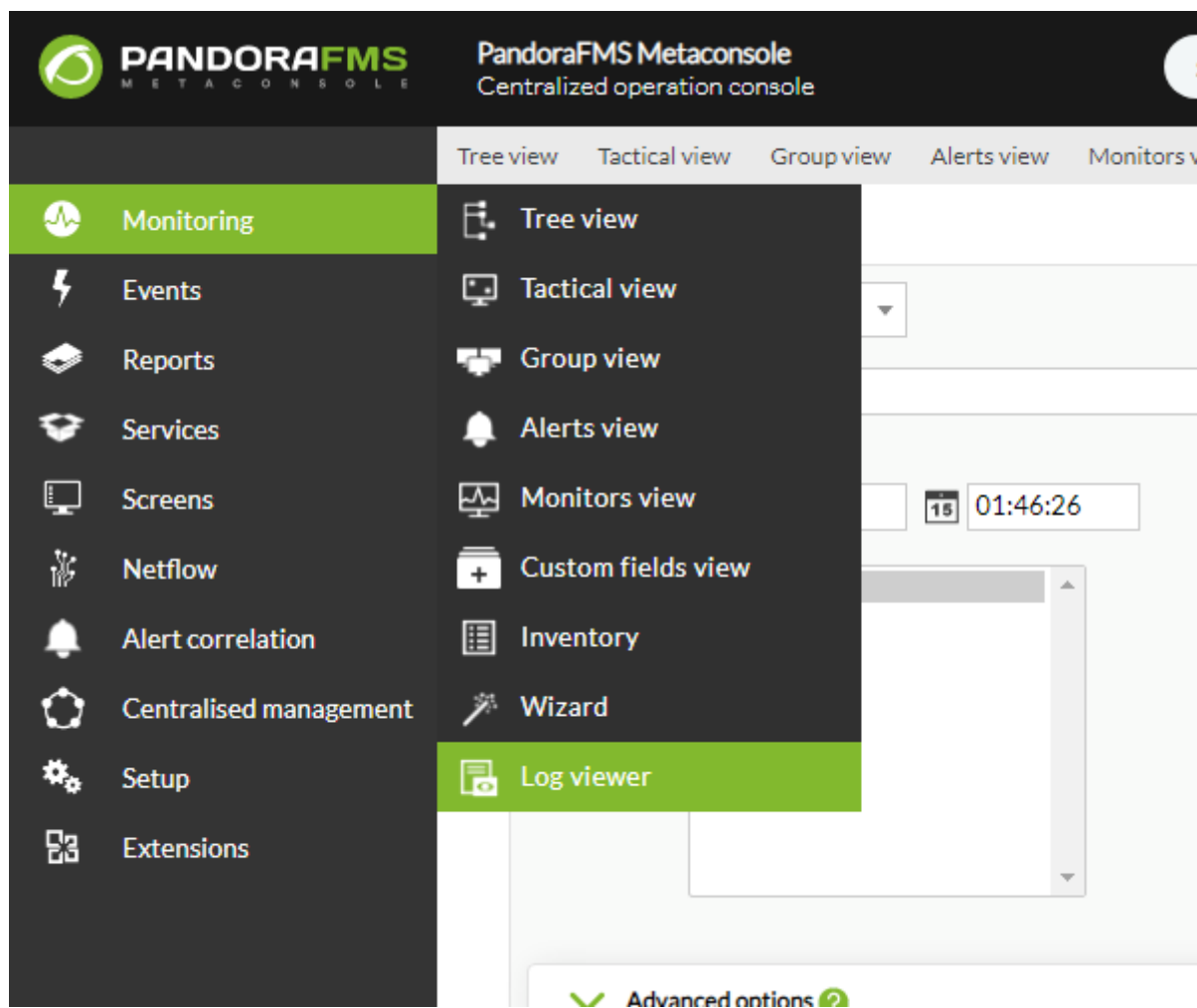
Module name	Data	Treshold	Current interval	Timestamp	Status
Network Traffic (Incoming)	184,738	N/A - 0/900K	300	4 minutes 30 seconds	●
Network Traffic (Outgoing)	994,151	N/A - 0/900K	300	4 minutes 30 seconds	●

Central	stress_varian_751	127.0.0.1	varian	■
Central	stress_garosh_209	127.0.0.1	garosh	■
Central	stress_garosh_308	127.0.0.1	garosh	■
Central	stress_garosh_236	127.0.0.1	garosh	■
Central	stress_varian_850	127.0.0.1	varian	■
Central	stress_varian_1093	127.0.0.1	varian	■
Central	stress_varian_210	127.0.0.1	varian	■
Central	stress_varian_1243	127.0.0.1	varian	■
Central	stress_varian_229	127.0.0.1	varian	■
Central	stress_garosh_681	127.0.0.1	garosh	■
Central	stress_varian_1143	127.0.0.1	varian	■
Central	stress_varian_3	127.0.0.1	varian	■
Central	stress_garosh_691	127.0.0.1	garosh	■
Central	stress_varian_256	127.0.0.1	varian	■

Showing 1 to 15 of 236 entries

Log viewer

NG 747 version or later.



You may find the log viewer in the monitoring section of the top menu. The view will be similar to that of the nodes, but including an extra multiple selector to select the logs collected by specific nodes. In the following [link](#) you may see the full description of parameters regarding this view in the node and which are saved in the Metaconsole.

To have access to this view, first enable it in the [general configuration of the Metaconsole](#) and configure the connection to Elasticsearch server, as it is described in the [Log Viewer configuration](#) section.

Then you may access the menu Monitoring → Log viewer, and you may select the filtering (Start date) of the last hour, the last 6 hours, and so on or choose within a date range (Select dates by range):



Search mode: Order:

Search: Group:

Select dates by range:

Server:


[Advanced options ?](#)

Start date:



- custom
- 1 hour
- 2 hours
- 6 hours**
- 12 hours
- 1 day

All nodes

Search mode: Order:

Search:  Group:

Select dates by range:

Start date:  End date: 

Server

[> Advanced options !\[\]\(863dadf657ea0c2f199e9bd573211810_img.jpg\)](#)

All
nod

Events

The screenshot displays the PandoraFMS Metaconsole interface. The top header includes the PandoraFMS logo and the text "PandoraFMS Metaconsole Centralized operation console". A search bar is visible on the right. The left sidebar contains a navigation menu with the following items: Monitoring, Events (highlighted in green), Reports, Services, Screens, Netflow, Alert correlation, Centralised management, Setup, and Extensions. The main content area shows a "Filter" section with buttons for "Current filter" (Not set), "Event", "Duplicated", and "Group events". Below this, it displays "Total Events per node: (100000)". A "Show 500 entries" dropdown is present. The event list table has columns for "Custom data", "Timestamp", and "Event n". A visible entry shows a timestamp of "1 minutes 31 seconds" and a partial event description: "Configura tend/sys 2 [kthrea D /usr/sbi DFOREG rocess! |".

Pandora FMS uses an event system to show that takes place in the monitored systems. In an event viewer, it is shown when a monitor is down, an alert has been triggered, or when the Pandora FMS system itself has some problem.

The Metaconsole has its own event viewer where the events from the associated instances are centralized. It is possible to centralize the events of all instances or just part of them. When the events of one instance are replicated in the metaconsole, its management becomes centralized in the metaconsole, so its display in the instance will be restricted to only reading.

Instance event replication to the Metaconsole

In order for the instances to replicate their events to the Metaconsole, it would be necessary to configure them one by one. To get more information about its configuration go to the section [Metaconsole Setup and configuration](#) in this manual.

Event Management

The event management display view is divided in the view and its configuration.

See Events

Event view

The normal event view, non-validated events of less than 8 hours, is accessed by clicking on the Events icon from the Metaconsole main page.

PandoraFMS Metaconsole
Centralized operation console

Search

Events

Events list

Filters: Current filter: Not set. Event status: Not validated. Max. hours old: Last 8 hours. Duplicated: Group events

S	Event name	Status	Agent name	Timestamp	Options
	(2) Warmup mode for unknown modules ended.	★		3 hours	<input type="checkbox"/>
	(2) Warmup mode for unknown modules started.	★		3 hours	<input type="checkbox"/>
	(2) meta-pandorafms predictionserver going UP	★		3 hours	<input type="checkbox"/>
	(2) meta-pandorafms eventserver going UP	★		3 hours	<input type="checkbox"/>
	(2) meta-pandorafms provisioningserver going UP	★		3 hours	<input type="checkbox"/>
	(2) meta-pandorafms migrationserver going UP	★		3 hours	<input type="checkbox"/>
	nodo-1-pandorafms icmpserver going DOWN	★		4 hours	<input type="checkbox"/>
	nodo-1-pandorafms snmpserver going DOWN	★		4 hours	<input type="checkbox"/>
	nodo-1-pandorafms dataserver going DOWN	★		4 hours	<input type="checkbox"/>
	nodo-1-pandorafms networkserver going DOWN	★		4 hours	<input type="checkbox"/>

Previous 1 2 3 4 Next 10

In progress selected

Execute event response

Event filter editing and creation **works the same way as that of nodes**. The event view filter default values are:



Filter

Group

Event type

Event status

Max. hours old

Duplicate

Free search

Severity
Critical
Critical/Normal

Group recursion

Search in secondary groups

Advanced options

The only difference with event filters on nodes is the Server field which allows you to choose the Metaconsole and/or one or more nodes.

Advanced options

Source

Extra ID

Comment

Agent search  

Server
koldo_server
Metaconsola
stod

User ack.

Alert events

Id source event

From (date:time) :

To (date:time) :

Custom data filter

Custom data search

Events with the following tags

configuration	None
cpu_usage	
critical	
disk_rate	
disk_usage	
dmz	
dmz test	
memory_usag	
network	
network_usag	

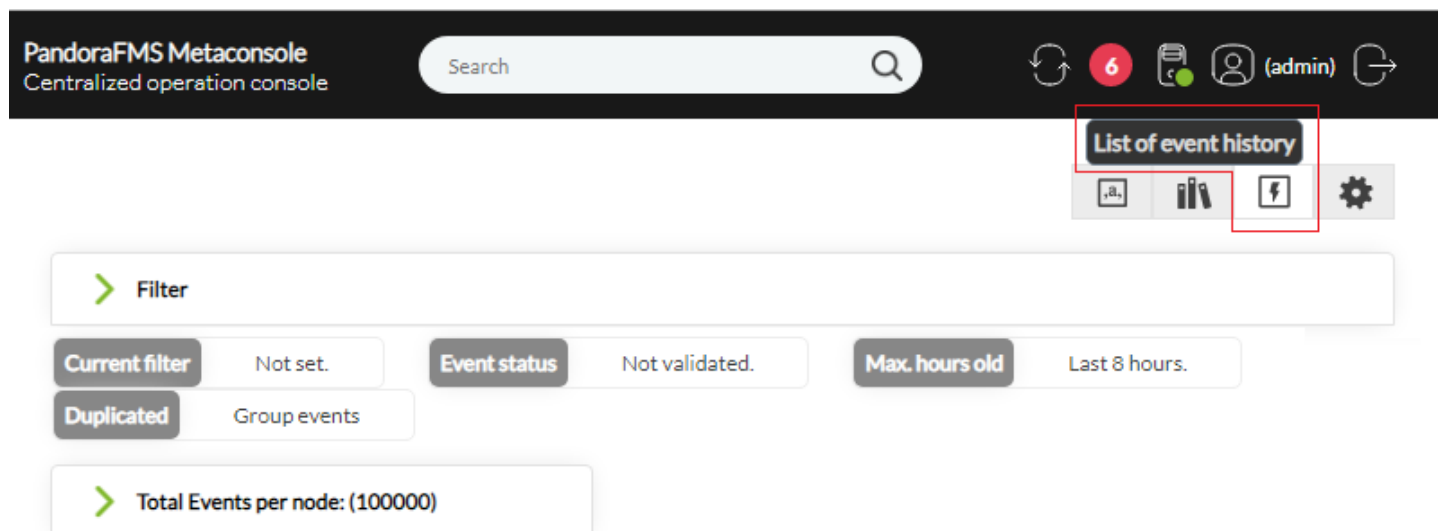
Events without the following tags

configuration	None
cpu_usage	
critical	
disk_rate	
disk_usage	
dmz	
dmz test	
memory_usag	
network	
network_usag	

When upgrading to version 767 the previously created filters may be unconfigured in the Server section, if so reconfigure your server preferences for each filter and save again to fix.

Event History

In order to have an event history, activate and configure this option in ►Setup → Metasetup → Performance and then the oldest events from some time ago (configurable), that have not been validated, will become part of a secondary view automatically: The event history view. This view is similar to the normal event view, and you can have access to it from a tab in the event view.

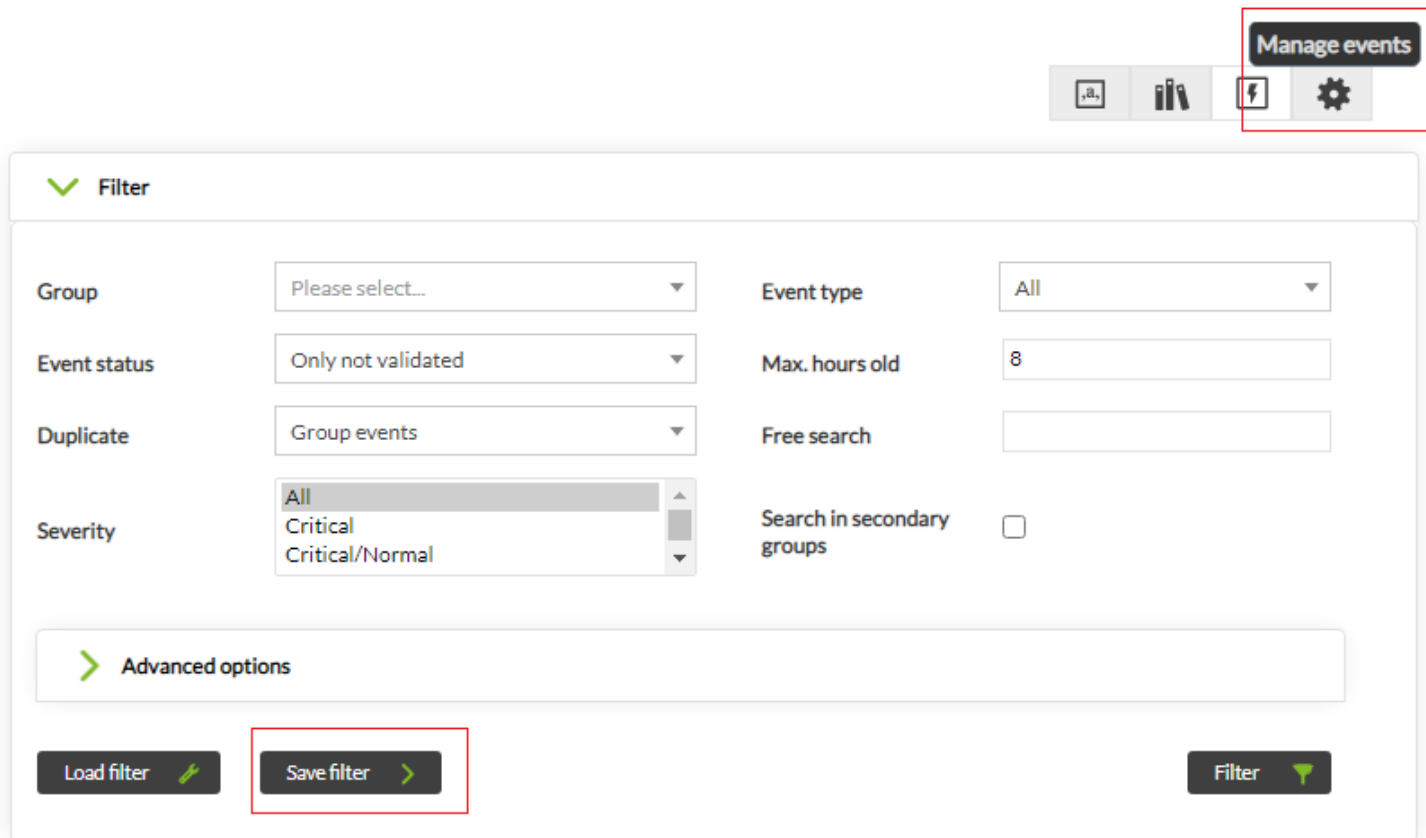


The screenshot displays the PandoraFMS Metaconsole interface. At the top, there is a navigation bar with the text "PandoraFMS Metaconsole" and "Centralized operation console". A search bar is located in the center of the navigation bar. On the right side of the navigation bar, there are several icons: a refresh icon, a notification icon with the number "6", a document icon, a user profile icon labeled "(admin)", and a back arrow icon. Below the navigation bar, there is a "List of event history" tab highlighted with a red box. Below the tab, there are several filter buttons: "Current filter" (Not set.), "Event status" (Not validated.), "Max. hours old" (Last 8 hours.), and "Duplicated" (Group events). At the bottom of the filter section, there is a button labeled "Total Events per node: (100000)".

Event Filter

The event views have a range of filtering options available to meet the user needs.

Filtering options can be created in two different ways. One of them is doing the filtering in the event view itself, and saving the selected filter afterwards by clicking Save filter.



The screenshot displays the Pandora FMS interface, specifically the 'Filter' section. At the top right, a 'Manage events' button is highlighted with a red box. Below this, the 'Filter' section is visible, containing several configuration options:

- Group:** Please select...
- Event status:** Only not validated
- Duplicate:** Group events
- Severity:** All, Critical, Critical/Normal
- Event type:** All
- Max. hours old:** 8
- Free search:** (empty text box)
- Search in secondary groups:**

Below the filter settings, there is an 'Advanced options' section. At the bottom of the filter section, there are three buttons: 'Load filter' (with a green arrow icon), 'Save filter' (with a green arrow icon and highlighted with a red box), and 'Filter' (with a green arrow icon).

The other way consists of going to ►Manage Events → Filter List → Create new filter and creating the desired possible filters manually. Later, the created filters must be loaded in the event filter options.



Create Filter

Filter name

Save in group ?

Group

Event type

Severity
 All
 Critical
 Critical/Normal
 Informative
 Maintenance
 Major
 Minor
 Normal
 Not normal
 Warning

Event status

Free search

Agent search ? ?

Block size for pagination

Max. hours old

User ack. ?

Duplicate

From (date)

To (date)

Events with the following tags

+

-

Events without the following tags

+

-

Alert events

Source

Extra ID

Comment

Custom data filter type

Custom data

Id souce event

Create >

Advanced event filter options

✓ **Advanced options**

<p>Source <input type="text"/></p> <p>Comment <input type="text"/></p> <p>Server <div style="border: 1px solid #ccc; padding: 2px; display: inline-block;"> koldo_server Metaconsola stod_server </div></p> <p>Alert events <input type="text" value="All"/></p> <p>From (date:time) <input type="text"/> : <input type="text" value="00:00:00"/></p> <p>Custom data filter <input type="text" value="Filter custom data by field name"/></p> <p>Events with the following tags</p> <div style="display: flex; align-items: flex-start;"> <div style="border: 1px solid #ccc; padding: 2px; margin-right: 5px;"> configuration cpu_usage critical disk_rate disk_usage dmz dmz test memory_usage network network_usage </div> <div style="margin: 0 5px;"> > < </div> <div style="border: 1px solid #ccc; padding: 2px; flex-grow: 1;"> None </div> </div>	<p>Extra ID <input type="text"/></p> <p>Agent search <input type="text"/> 🔍 ⓘ</p> <p>User ack. <input type="text" value="Any"/></p> <p>Id source event <input type="text" value="0"/></p> <p>To (date:time) <input type="text"/> : <input type="text" value="00:00:00"/></p> <p>Custom data search <input type="text"/></p> <p>Events without the following tags</p> <div style="display: flex; align-items: flex-start;"> <div style="border: 1px solid #ccc; padding: 2px; margin-right: 5px;"> configuration cpu_usage critical disk_rate disk_usage dmz dmz test memory_usage network network_usage </div> <div style="margin: 0 5px;"> > < </div> <div style="border: 1px solid #ccc; padding: 2px; flex-grow: 1;"> None </div> </div>
--	--

Some important fields of the advanced event filter:

- **Agent search:** It allows you to search only for specific agents, you must enter at least two characters to display the corresponding list.
- **Server:** It allows you to choose the node(s) and/or Metaconsole containing the events.
- **User ack.:** It allows you to select a user and their validations performed.
- **Events with the following tags y Events without the following tags:** Respectively, they allow you to select the events that have or do not have certain tags.
- **Custom data filter:** You can filter by custom fields using the fields Custom data filter, either by filtering the field name (Filter custom data by field name) or by custom field content (Filter custom data by field value). These fields will be displayed as columns in the event view.

User ack.

Alert events

From (date:time)

To (date:time)

Custom data filter

Custom data search

Events with the following tags

Event Details

In the event list (normal or from history) it is possible to see the details of one event clicking on the event name or in the 'Show more' icon from the action field.

Custom data	S Timestamp	Event name	Agent ID	Status	Agent name	Event Id	Options	
	Now	Module 'Connections opened' is going to WARNING (421)	106	★	koldo. 32	3400 9449	🔍 ✓ ⌛ 🗑️	☐
	Now	Module 'Connections opened' is going to WARNING (412)	113	★	koldo. 39	3400 9454	🔍 ✓ ⌛ 🗑️	☐
	Now	Module 'Connections opened' is going to CRITICAL (464)	107	★	koldo. 33	3400 9449	🔍 ✓ ⌛ 🗑️	☐
	Now	Module 'Connections opened' is going to WARNING (405)	109	★	koldo. 35	3400 9452	🔍 ✓ ⌛ 🗑️	☐

The fields of one event are shown in a new window with several tabs.

General

Module 'Network Traffic (Incoming)' is going to CRITICAL (947293)



General

Details

Agent fields

Comments

Responses

Event ID	#34009425	
Event name	Module 'Network Traffic (Incoming)' is going to CRITICAL (947293)	
Node	koldo_server	
Timestamp	August 2, 2022, 3:45 am	
Owner	N/A	
Type	Going up to critical state	
Duplicate	No	
Severity	Critical	
Status	New event	
Acknowledged by	N/A	
Group	Servers	
Contact	N/A	
Tags	N/A	
Extra ID	N/A	
Module custom ID	N/A	

The first tab shows the following fields:

- Event ID: It is an unique identifier for each event.
- Event Name: It is the event name. It includes a description.
- Date and Hour : Date and Time when the event is created in the event console.
- Owner: Name of the user owner of the event
- Type: Type of event. There can be the following types: Ended Alert, Fired Alert, Retrieved Alert, Configuration change, Unknown, Network system recognized by the recon, Error, Monitor in Critical status, Monitor in Warning status, Monitor in Unknown status, Not normal, System and Manual validation of one alert.
- Repeated: It defines whether the event is repeated or not.
- Severity: It shows the severity of the event. There are several levels: Maintenance, Informative, Normal, Minor, Warning, Major and Critical
- Status: It shows the status of the event. There are different status: New, Validated and In process
- Validated by: If the event has been validated, it shows the user who validated it, and the date and when when it happened.
- Group: If the event comes from an agent module, it shows the group the agent belongs to.
- Tags: If the event comes from an agent module, it shows the module tags.
- Extra ID: Extra ID that is assigned to the event to be able to look for it as free text.

Details

Module 'Network Traffic (Incoming)' is going to CRITICAL (947293) ✕

General



Details

Agent fields

Comments

Responses

Agent details

Name	koldo.228
IP Address	N/A
OS	 Linux (2.6)
Last contact	2 minutes 07 seconds
Last remote contact	August 2, 2022, 3:45 am
Custom fields	View custom fields >
Module details	
Name	Network Traffic (Incoming)
Module group	Not assigned
Graph	
Alert details	N/A
Instructions	N/A
Extra ID	N/A
Source	monitoring_server

The second tab shows details of the agent and the module that created the event. It is also possible to have access to the module graph.

The last data is the source of the event, which could be a Pandora FMS server or any source when the API is used to create the event.

Agent Fields

Module 'Network Traffic (Incoming)' is going to CRITICAL (947293) ✕

⚡ General

🔍 Details

📄 Agent fields

✍ Comments

👤 Responses

Serial Number	N/A
Department	N/A
Additional ID	N/A
eHorusID	N/A
vmware_vcenter_ip	N/A
vmware_datacenter	N/A
vmware_user	N/A
vmware_pass	N/A
vmware_type	N/A
vmware_parent	N/A

The third flap shows the Agent custom fields.

Comments

Module 'Network Traffic (Incoming)' is going to CRITICAL (947293) ✕

⚡ General

🔍 Details

📄 Agent fields

✍ Comments

👤 Responses

[Add comment >](#)

Added comment by admin (#34009425)

August 2, 2022, 3:58 am Test for documentation.

The fourth tab shows the comments that have been added to the event and the modifications resulting from the change of owner or the event validation.

Event Responses

Module 'Network Traffic (Incoming)' is going to CRITICAL (947293) ✕

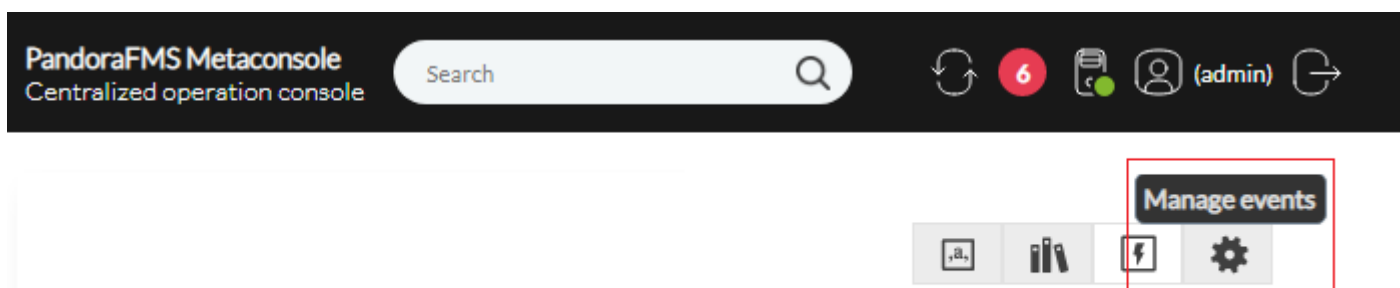
General	Details	Agent fields	Comments	Responses
Change owner	None			Update >
Change status	New			Update >
Comment				Add comment >
Delete event				Delete event ✕
Custom responses	Ping to host			Execute >
Description	Ping to the agent host			

The fifth tab shows actions or responses that could be performed on the event. The actions to be carried out are the following:

- Changing the owner
- Changing the status
- Adding a comment
- Deleting the event
- Executing a custom response: It would be possible to execute all the actions that the user has configured.

Configure Events

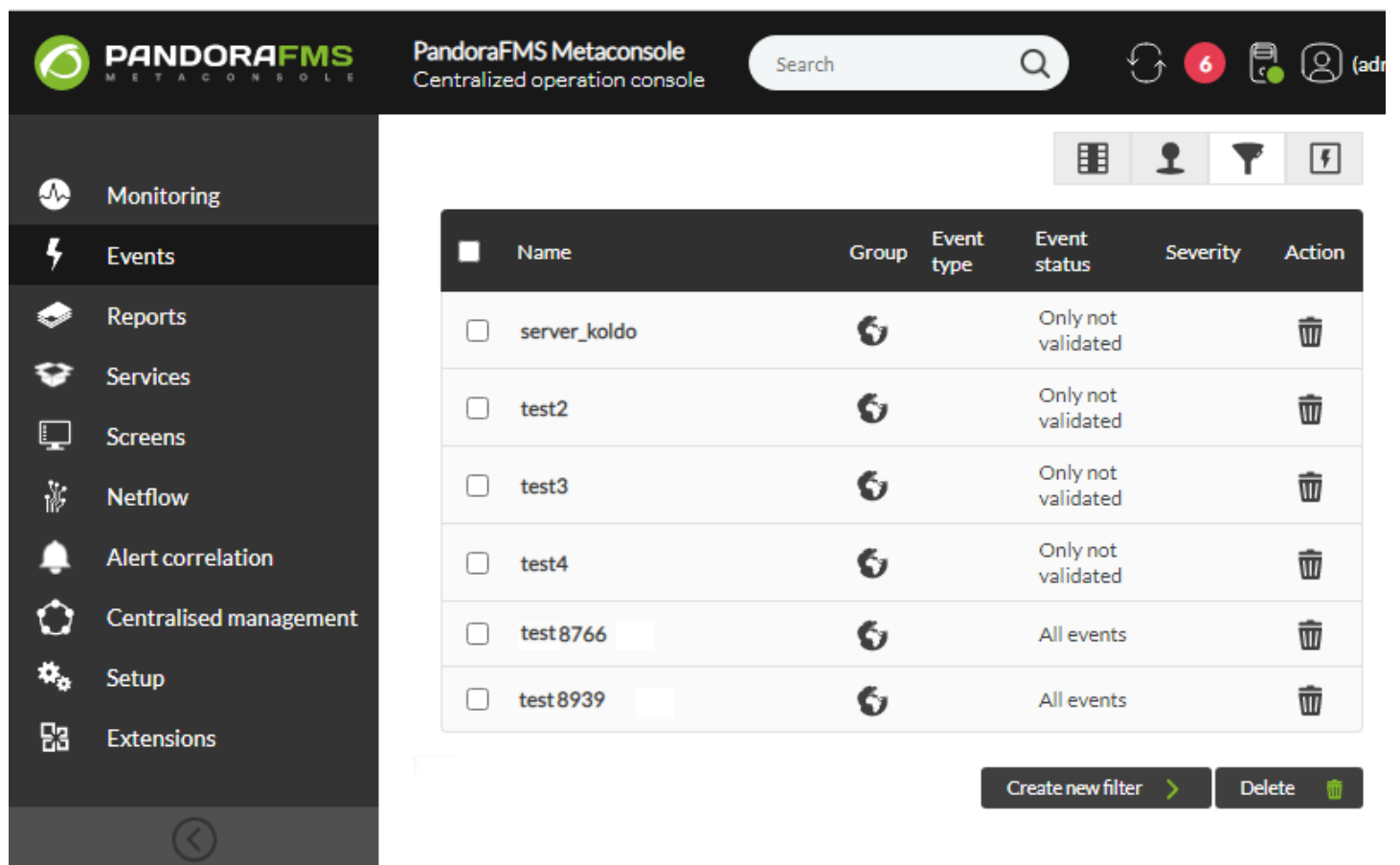
Users with ACLs EW bits will have a tab to access the event configuration panel available.



Manage Event Filters

Filters on events allow to parametrize the events that you want to see in the event console. With Pandora FMS, it is possible to create predefined filters so that one or several users can use them.

Filters can be edited by clicking on the filter name.



The screenshot displays the PandoraFMS Metaconsole interface. The top navigation bar includes the PandoraFMS logo, the text "PandoraFMS Metaconsole Centralized operation console", a search bar, and several utility icons. A left sidebar contains a menu with options: Monitoring, Events, Reports, Services, Screens, Netflow, Alert correlation, Centralised management, Setup, and Extensions. The main content area shows a table of filters with the following columns: Name, Group, Event type, Event status, Severity, and Action. The table contains seven rows of filter data. Below the table are two buttons: "Create new filter" and "Delete".

<input type="checkbox"/>	Name	Group	Event type	Event status	Severity	Action
<input type="checkbox"/>	server_koldo			Only not validated		
<input type="checkbox"/>	test2			Only not validated		
<input type="checkbox"/>	test3			Only not validated		
<input type="checkbox"/>	test4			Only not validated		
<input type="checkbox"/>	test8766			All events		
<input type="checkbox"/>	test8939			All events		

In order to create a new filter, click on the button "create filters". There, it will show a window where the filter values are configured.



Create Filter

Filter name

Save in group (i)

Group

Event type

Severity

Event status

Free search

Agent search (i)

Block size for pagination

Max. hours old

User ack. (i)

Duplicate

From (date)

To (date)

Events with the following tags

Events without the following tags

Alert events

Source

Extra ID

Comment

Custom data filter type

Custom data

Id souce event

Create >

The fields through which filtering is performed are these:

- Group: Combo where you can select the Pandora FMS group.
- Event Type: Combo where you can select the event type.
- Severity: Combo where you can select by event severity.
- Event Status: Combo where you can select by event status.
- Free search: Field that allows text free searching.
- Agent Search: Combo where you can select the source agent of the event.
- Max hour old: Combo where the hours are shown.
- User Ack: Combo where you can select among the users that have validated an event.
- Repeated: Combo where you can choose between being shown the repeated events or all events

Besides the search fields in the Event Control filter menu, there is the Block size for pagination option, where you can select the number of event that will be found in each page when paging.

Manage Responses

In events, responses or actions to be taken in some specific event can be configured. For example, sending a *ping* to the agent IP which generated the event, connecting through SSH with this agent, etc.

The screenshot shows the PandoraFMS Metaconsole interface. The top header includes the PandoraFMS logo, the text 'PandoraFMS Metaconsole Centralized operation console', and a search bar. The left sidebar contains navigation icons and labels for Monitoring, Events, Reports, Services, Screens, Netflow, Alert correlation, Centralised management, Setup, and Extensions. The main content area displays a table of responses with the following data:

Name	Description	Group	Actions
Ping to host	Ping to the agent host		
Create incident from event	Create a incident from the event with the standard incidents system of Pandora FMS		
Restart agent	Restart the agent with using UDP protocol. To use this response is necessary to have installed Pandora FMS server and console in the same machine.		
Ping to module agent host	Ping to the module agent host		
echo test	test		

At the bottom right of the table area, there is a 'Create response' button with a right-pointing arrow.

The response configuration allows to configure both a command and a URL.



Edit event responses

Name Group All ▾

Description

Location i Modal window ▾ Size Width (px) Height (px)

Parameters Type Command ▾

Command ?

Display command i

Create >

To this effect, define a list of parameters separated by commas that will be filled in by the user when the response is executed. You can also use both the event's internal macros and those within this list:

- `_agent_address_` : Agent address.
- `_agent_id_` : Agent ID.
- `_alert_id_` : Event related alert ID.
- `_event_date_` : Date on which the event occurred.
- `_event_extra_id_` : Extra ID.
- `_event_id_` : Event ID.
- `_event_instruction_` : Event instructions.
- `_event_severity_id_` : Event severity ID.
- `_event_severity_text_` : Event severity (translated by Pandora FMS console).
- `_event_source_` : Event source.
- `_event_status_` : Event status (new, validated or event in process).


- `_event_tags_` : Event tags separated by commas.
- `_event_text_` : Full text of the event.
- `_event_type_` : Event type (System, going into Unknown Status...).
- `_event_utimestamp_` : Date on which the event took place in utimestamp format.
- `_group_id_` : Group ID.
- `_group_name_` : Group name in database.
- `_module_address_` : Event associated module address.
- `_module_id_` : Event associated module ID.
- `_module_name_` : Event associated module name.
- `_owner_user_` : Event owner user.
- `_user_id_` : User ID.
- `_current_user_` : Id of the user who triggers the response.
- Custom event fields are also available in event response macros. They have `_customdata_*_` form, where the asterisk (*) must be replaced by the custom field key you wish to use.
 - `_customdata_X_` : Pulls a particular field from custom data, replacing the X with the field's name.
 - `_customdata_text_` : Pulls all information from custom data in text mode.
 - `_customdata_json_` : Pulls all information from custom data in JSON format.

Customize Fields in the Event View

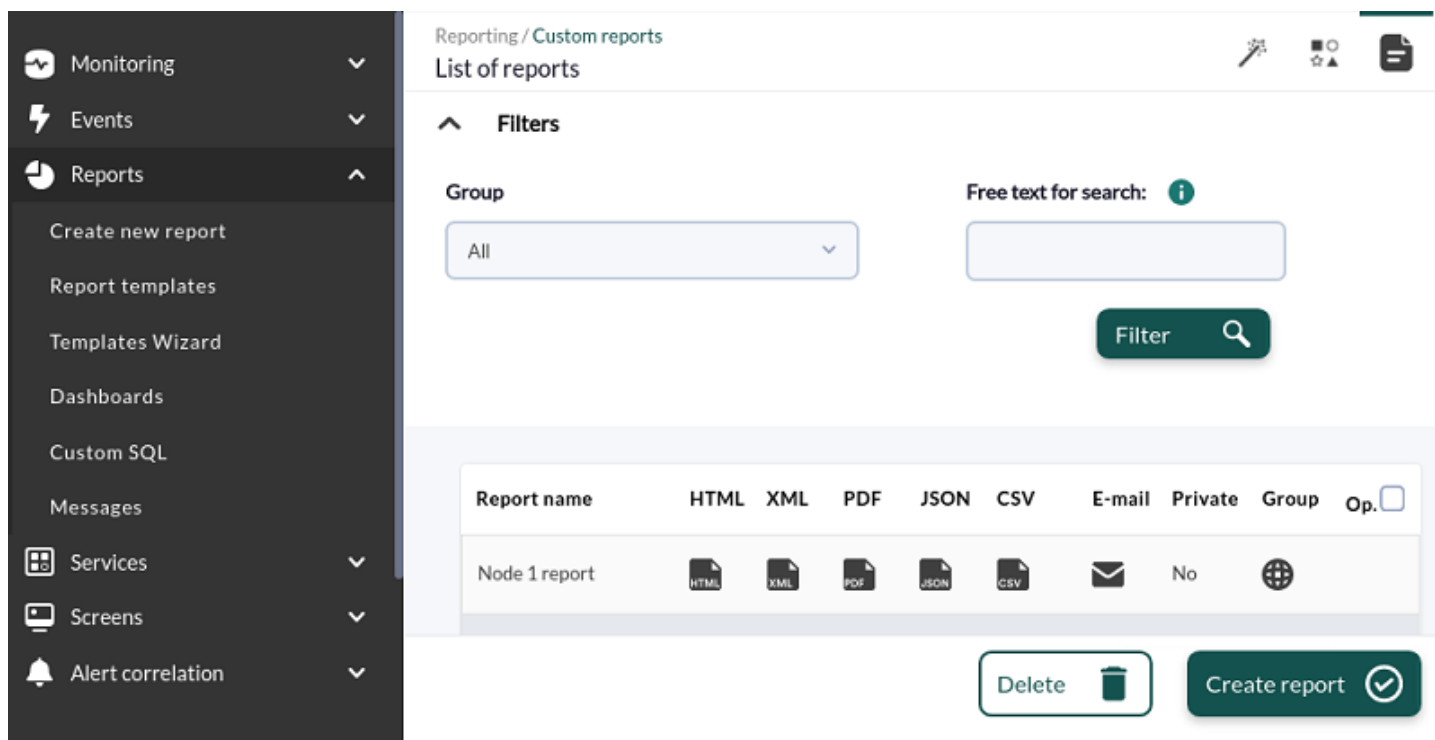
With Pandora FMS, it is possible to add or delete columns in the Event View. Each column is a field for event information, so it is possible to customize that view.

The screenshot shows the PandoraFMS Metaconsole interface. The top navigation bar includes the PandoraFMS logo, the text 'PandoraFMS Metaconsole Centralized operation console', and a search bar. The left sidebar contains navigation icons and labels for Monitoring, Events, Reports, Services, Screens, Netflow, Alert correlation, Centralised management, Setup, and Extensions. The main content area is titled 'SHOW EVENT FIELDS' and features a configuration panel with two columns: 'Fields available' and 'Fields selected'. The 'Fields available' list includes Agent IP, User, Group, Event Type, Module Name, Alert, Severity, Comment, Tags, and Source. The 'Fields selected' list includes Custom data, Severity mini, Timestamp, Event name, Agent ID, Status, Agent name, and Event Id. A green arrow points from the 'Fields available' list to the 'Fields selected' list. An 'Update' button is located at the bottom right of the configuration area.

- From this screen, you may add fields to the Event View by moving them from the Fields available box, to the left box, Fields selected, using the horizontal arrow.

- To remove fields from the Event View, move them from the right box to the left box using the horizontal arrow.
- You may also change the order of the fields in the Field selected by selecting them one by one and clicking on the vertical arrows below the list.
- To restore the fields to how they were before the modification, click on the icon .

Reports



Reporting / Custom reports

List of reports

Filters

Group: All

Free text for search:

Filter

Report name	HTML	XML	PDF	JSON	CSV	E-mail	Private	Group	Op.
Node 1 report							No		

Delete

Create report

In the Metaconsole, it is possible to do all kinds of reports on Instance data. The configuration of one report is stored in the Metaconsole, but when it is displayed, it retrieves data by connecting to the instances.

For the report editor, the source of agents and monitors is visible. However, the user will not know from which Instance they come from.

Reports can be created in two different ways:

- Manually
- With report templates

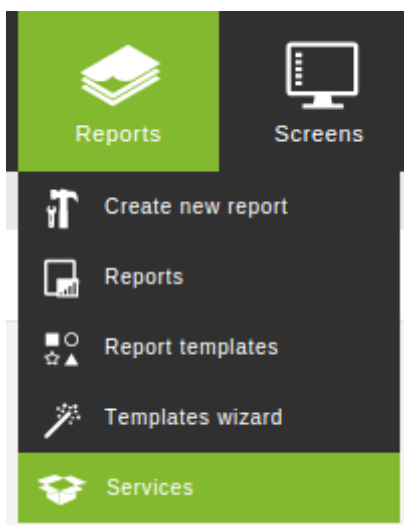
To find out more visit the [Reports](#) section from this documentation.

Metaconsole service monitoring

As seen in-service monitoring on nodes, a service is an IT resource group sorted out by its features.

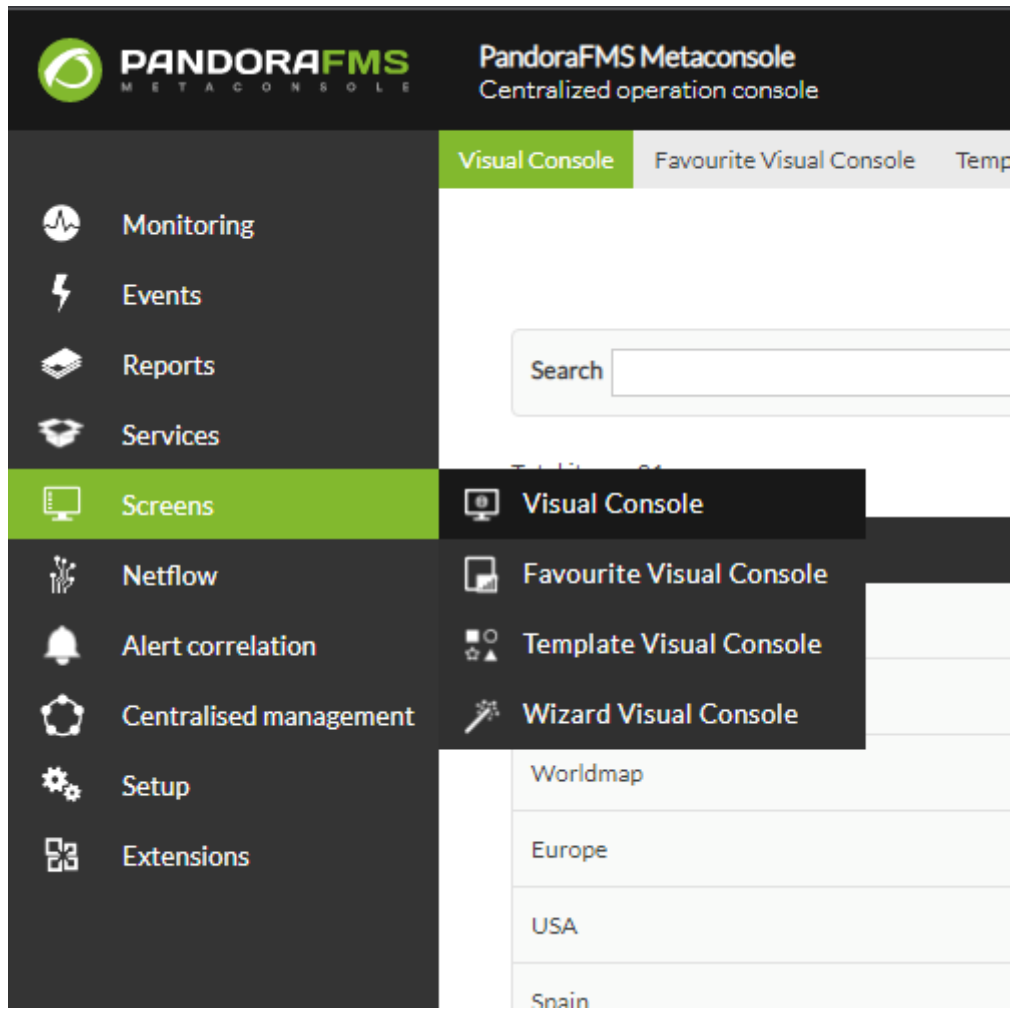
With service monitoring in the Metaconsole, the services present in the nodes can be grouped and all the infrastructure status can be checked at a glance.

They can be added in the Metaconsole in the following way: - Select the “Reports” → “Services” option



To find out more about creating services and configuring them, visit the Service section in the following [link](#).

Screens



To enable these menus, check the [Metaconsole's general setup](#).

Visual Console

A visual console can be configured in the Metaconsole, which is a panel consisting of a background and elements placed on it.

Data view and configuration are exactly the same as those of the visual maps in the usual console, but data is retrieved from the Instances in a transparent way for the user.

PANDORAFMS META CONSOLE
PandoraFMS Metaconsole
Centralized operation console

Search 6 (admin)

Visual Console | Favourite Visual Console | Template Visual Console | Wizard Visual Console

Monitoring
Events
Reports
Services
Screens
Netflow
Alert correlation
Centralised management
Setup
Extensions

Search Group **All** Group Recursion Search

Total items: 21

Map name	Group	Items	Copy	Delete
Demo visual console		47		
Demo visual console 2		13		
Worldmap		9		
Europe		14		
USA		15		
Spain		19		
Madrid		20		
Germany		15		

All this information is in the section of node [Visual Maps](#).

NetFlow

The screenshot shows the PandoraFMS Metaconsole interface. The top header includes the PandoraFMS logo, the text 'PandoraFMS Metaconsole Centralized operation console', a search bar, and several utility icons. A sidebar on the left contains navigation links: Monitoring, Events, Reports, Services, Screens, Netflow (highlighted), Alert correlation, Centralised management, Setup, and Extensions. The main content area is titled 'Live view' and 'Filters'. A 'Draw live filter' dialog box is open, showing the following configuration: Connection: koldo_server; Start date: 2022/08/02 (with a '1 day' interval dropdown); End date: 2022/08/03 00:03:43; Resolution: Medium; Max. values: 10; Aggregate by: DST IP address. At the bottom of the dialog, there is an 'Advanced' section and two buttons: 'Draw' and 'Save as a new filter'.

To be able to have this option available in the Metaconsole, the section view must be activated within the Metasetup [general option](#) in the Metaconsole. At the same time, to be able to carry out a node NetFlow from the Metaconsole, the node must have NetFlow activated in its setup.

To learn more about how to carry out the live view, the possible NetFlow filters, as well as how to install necessary dependencies, visit the NetFlow section [through this link](#).

Node information flow can only be obtained one at a time. Information from more than one node cannot be obtained simultaneously.

[Go back to Pandora FMS documentation index](#)