

Visualisation



om:

<https://pandorafms.com/manual/!776/>

Permanent link:

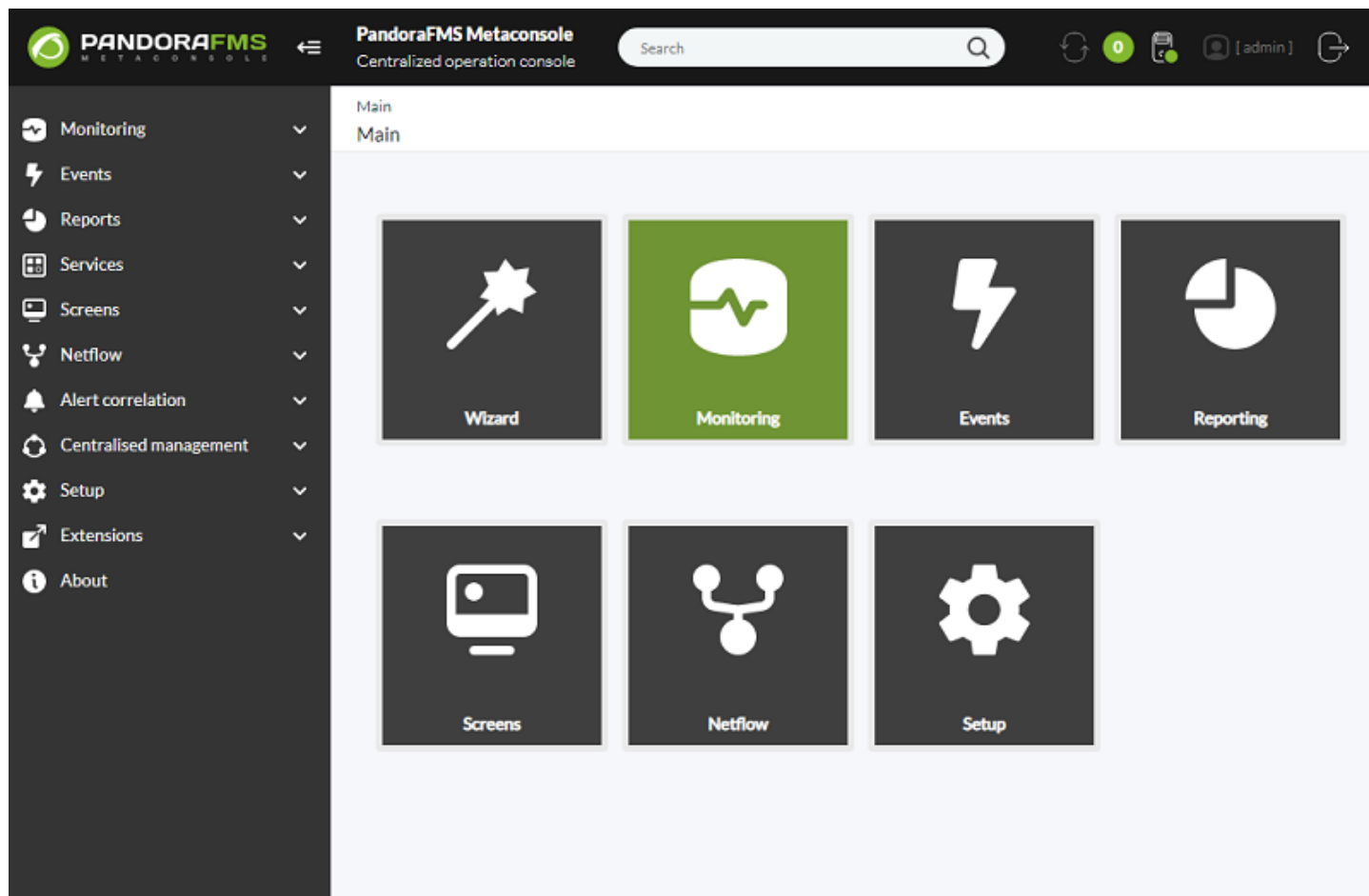
https://pandorafms.com/manual/!776/fr/documentation/pandorafms/command_center/05_visualization

2024/06/10 14:34



Visualisation

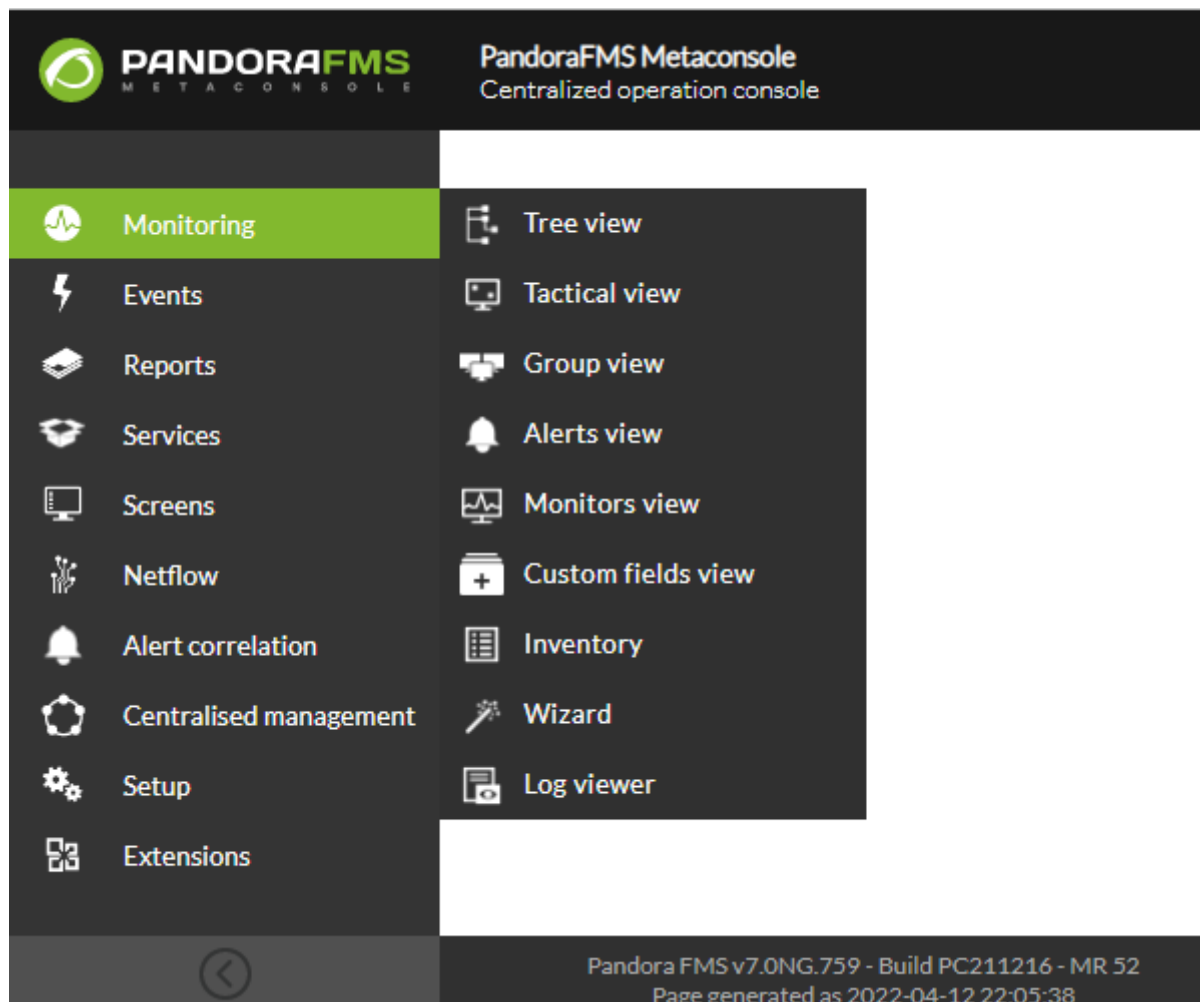
E Cette section explique les options de la Métaconsole dédiées à la navigation et à la visualisation des données des agents, modules et alertes des instances attachées à une Métaconsole.



Supervision

E Il existe plusieurs façons de visualiser les données :

- Vue de l'arbre (Tree view).
- Vue tactique (Tactical view).
- Vue de groupe (Group view).
- Vue des alertes (Alerts view).
- Vue de moniteurs (Monitor view).
- Vue des champs personnalisés (Custom fields view).
- Inventaire (Inventory).
- Assistant (Wizard).
- Viseur des journaux (Log viewer).



Vue de l'arbre

The screenshot displays the PandoraFMS Metaconsole interface. At the top, the header includes the PandoraFMS logo, the text "PandoraFMS Metaconsole Centralized operation console", a search bar, and user information for "admin". Below the header is a navigation menu with tabs: "Tree view" (selected), "Tactical view", "Group view", "Alerts view", "Monitors view", "Custom fields view", "Inventory", "Wizard", and "Log viewer". On the left side, there is a vertical sidebar with various icons representing different system components. The main content area shows a "Show Options" button at the top, followed by a list of "Groups found: 12". Each group is represented by an icon and a list of counts in brackets, color-coded by status: 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], and Workstations [17:16:1]. At the bottom of the interface, a footer contains the version information: "Pandora FMS v7.0NG.759 - Build PC211216 - MR 52" and the page generation timestamp: "Page generated as 2022-04-12 22:37:44".

Cette vue permet de visualiser les moniteurs des agents sous forme d'arborescence. Il est accessible via la Surveillance de la → Vue d'arbre.

Vous pouvez filtrer par état du module (Critical, Normal, Warning et Unknown) et effectuer des recherches par nom d'agent ou par groupe. De plus, il existe la possibilité d'afficher ou non les agents ou modules non démarrés (options de case à cocher Show not init modules et Show not init agents), ainsi que d'afficher la hiérarchie complète.

Pour chaque niveau, un décompte du nombre d'éléments de votre branche est affiché : nombre total d'éléments, Critical (couleur rouge), Warning (couleur jaune), Unknown (couleur grise), modules non initiés (couleur bleue) et état normal (couleur verte).

Au début, le premier niveau est chargé. En cliquant sur les éléments de chaque niveau, la branche sera déployée avec les éléments qu'elle contient.

Il s'agit d'un arborescence de groupes où les agents sont affichés filtrés par le groupe auquel ils appartiennent.

The screenshot shows the Pandora FMS search interface. At the top, there is a 'Show Options' section with a green checkmark. Below this, there are two search input fields: 'Search group' and 'Search agent'. To the right of these fields are several checkboxes: 'Show not init modules' (checked), 'Show not init agents' (checked), and 'Show full hierarchy' (unchecked). There is also a dropdown menu for 'Agent status' set to 'All' and a 'Filter' button with a magnifying glass icon.

Below the search options, it says 'Groups found: 12'. A tree view shows the following structure:

- 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]

Les éléments affichés dans le groupe sont limités par les autorisations ACL et par les autorisations par Tags de l'utilisateur

Niveaux

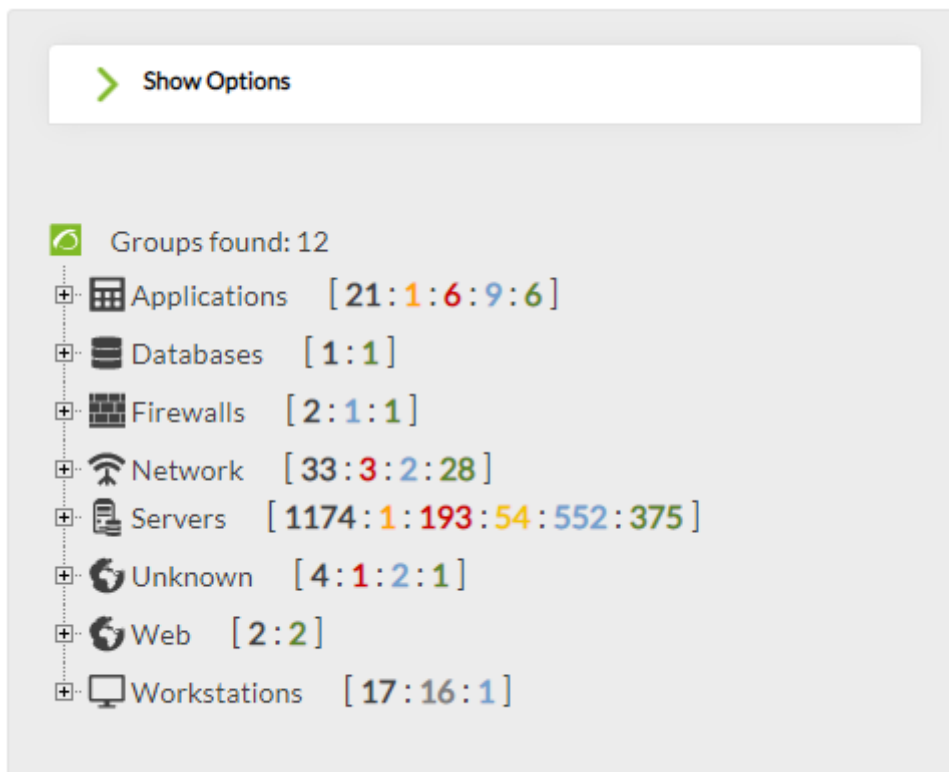
Groupes

C'est le premier niveau.

Lors du déploiement de la branche d'un groupe, les agents contenus dans le groupe apparaissent.

Le nombre à côté du nom du groupe fait référence au nombre d'agents qu'il contient et qui se trouvent dans chaque état.

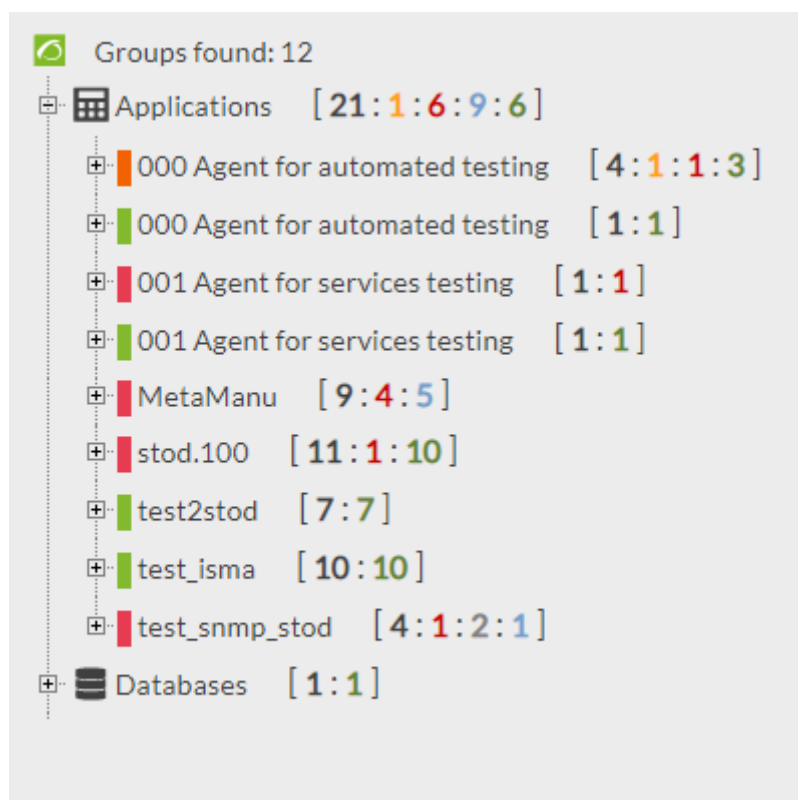
Seuls les agents actifs contenant au moins un module actif et en état de démarrage sont affichés.



Agents

Lors du déploiement de la branche d'un agent, les modules contenus dans l'agent apparaissent.

Le nombre à côté du nom du groupe fait référence au nombre d'agents qu'il contient et qui se trouvent dans chaque état.



Lorsque vous cliquez sur le nom de l'agent, des informations à son sujet s'affichent à droite : nom, adresse IP, date de la dernière mise à jour, système d'exploitation, ainsi qu'un graphique des événements et des accès des dernières 24 heures.

Pour que les données relatives aux champs personnalisés (*Custom Fields*) que peuvent avoir les agents puissent être affichées dans cette fenêtre d'information de la Métaconsole, vous devez activer sur les nœuds le jeton Display up front expliqué dans [la section suivante](#).

✕

✓ **Agent data**

Agent name	KOLDO_AGENT
IP Address	192.168.80.34 i
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: 5px; display: inline-block;">100%</div>

Go to agent edition ✎

✓ **Advanced information**

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

✓ **Agent access rate (24h)**

✓ **Events (24h)**

Modules

Le module est la dernière branche de l'arbre.

The screenshot shows a tree view of modules under the parent 'test_isma [10 : 10]'. The 'Windows version' module is selected, and its details are shown in a pop-up window on the right.

test_isma [10 : 10]	
AD AppMgmt	OK [Alert] [101]
BIOS Serial Number	System Serial [Magnifying Glass] [Alert] [101]
Computer Chassis Bootup State	3 [Alert] [101]
Computer Daylight In Effect	True [Alert] [101]
Computer DNS Host Name	WIN- [Magnifying Glass] [Alert] [101]
Computer Front Panel Reset Status	3 [Alert] [101]
CPU load	10 [Alert] [101]
Perf_NTDSABBrowsec	0 [Alert] [101]
Total Virtual Memory Size	10,864,936 [Alert] [101]
Windows version	Microsoft Wi [Magnifying Glass] [Alert] [101]

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 [Refresh]

Go to module edition [Pencil]

En cliquant sur le nom du module, des informations spécifiques s'affichent à droite. À côté du nom de chaque module dans cette branche apparaîtront plusieurs boutons :

- Graphique du module : Une fenêtre contextuelle (*pop-up*) s'ouvre avec le graphique du module.
- Si le module a des alertes, une icône d'alerte s'affiche : En cliquant sur l'icône, vous verrez à droite des informations sur les alertes du module : les modèles auxquels ils correspondent et leurs actions.
- Si le module a une icône de loupe, cela indique que le texte de la dernière donnée reçue est très long et vous devrez cliquer dessus pour visualiser son contenu complet.
- Informations *brutes* : Vous accéderez à la vue du module où les données reçues sont affichées dans un tableau.

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

Vue tactique

La vue tactique de la Métaconsole se compose de :

- Tableau récapitulatif des états des agents et des modules.
- Tableau avec les derniers événements.
- Tableau avec la dernière activité dans les instances de 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
---	---	---	---

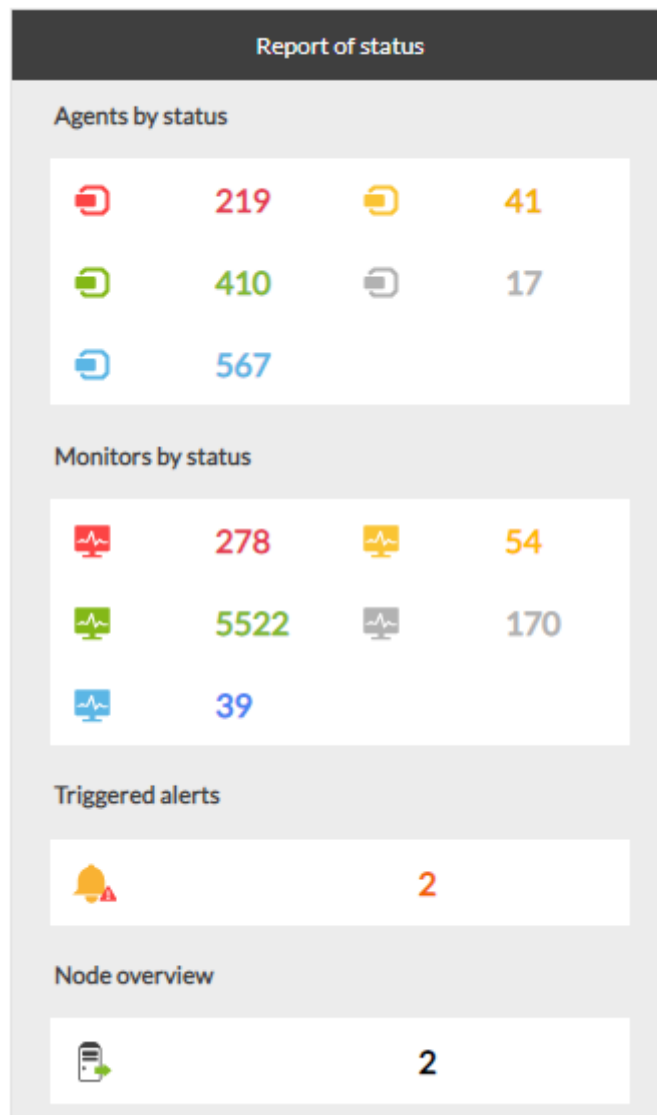
Info of status in events (1 hours)

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

Informations sur les agents et les modules



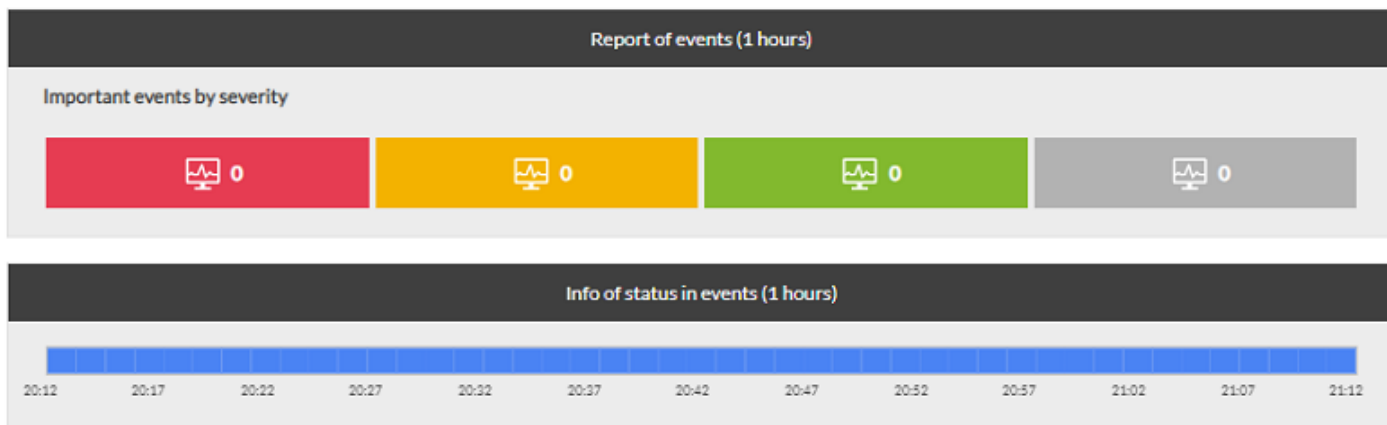
Le rapport d'état est affiché dans un tableau récapitulatif :

- Agents par état.
- Moniteurs par état.
- Alertes déclenchées.
- Récapitulatif des nœuds.

À l'exception du résumé des nœuds, vous pouvez cliquer sur chaque valeur numérique pour en savoir plus sur chaque thème.

Derniers événements

Un tableau avec les événements de la dernière heure résumés dans les différents états de ces derniers (Critical, Warning, Normal et Unknown) est affiché d'une part. D'autre part, les mêmes événements de la dernière heure sont affichés par ordre d'arrivée à la Métaconsole (Info of status in events).



Cet vue est uniquement informative, il n'est pas possible de valider des événements ni de voir leurs informations étendues.

Vue des groupes

La vue de groupes est une table avec les groupes de chaque instance et les informations suivantes de chacun :

- Nom du groupe. Le premier est le groupe "Tous". Si des groupes secondaires sont utilisés, ils sont accompagnés d'une icône informative.
- Nombre total d'agents.
- L'état de ce groupe (le pire des états de ses agents).
- Nombre d'agents en état Inconnu.
- Nombre d'agents en état Non initié.
- Nombre d'agents en état *Critical*.
- Nombre de modules en état Inconnu.
- Nombre de modules en état Non initié.
- Nombre de modules en état Normal.
- Nombre de modules en état *Warning*.
- Nombre de modules en état *Critical*.
- Nombre d'alertes déclenchées.
- Nombre d'agents en état Normal.
- Nombre d'agents en état *Warning*.

Monitoring / Views

GROUP VIEW

Summary of the status groups

Agents

Modules

8.24%

1.43%

85.30%

3.94%

100%

1.02%

0.15%

89.97%

8.80%

0.06%

Total items: 11

Force	Group/Tags	Agents						Modules					
		Total	Unknown	Not initialised	Normal	Warning	Critical	Unknown	Not initialised	Normal	Warning	Critical	Alert triggered
<input checked="" type="radio"/>	<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			

Vue des alertes

La vue des alertes est un tableau récapitulatif avec les informations des alertes dans les instances où vous pouvez observer l'agent auquel elles appartient, leur module, le modèle utilisé, l'action utilisée et la dernière fois qu'elles ont été déclenchées.

PandoraFMS Metaconsole
Centralized operation console

Search

Refresh 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

Vue des moniteurs

La vue des moniteurs est une table contenant des informations sur les moniteurs des Instances.

Les modules affichés sont limités par les autorisations ACL et par les autorisations par *Tags* de l'utilisateur.

Elle peut être filtrée par :

- Groupe.
- État du module.
- Groupe du module.
- Nom du module.
- *Tags*.
- Recherche libre.
- Type de serveur.
- Type de donnée.

Tous les moniteurs peuvent être affichés, uniquement ceux qui sont actifs ou uniquement ceux qui sont désactivés.

✓ Show Options

Group:
 Monitor status:
 Module group:

Module name: ⓘ Search:
 Tags ⓘ: Show ⓘ

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	0		0/400 - 0/450	243 conns	Now
1	DATA	Dropped Bit...nothing		5 minutes	0		N/A - N/A	349,416,065[...] jins ⓘ	Now
1	DATA	Network Tra...coming)		5 minutes	0		N/A - 0/900K	213,017 [...]]sec ⓘ	Now
1	DATA	Network Tra...tgoing)		5 minutes	0		N/A - 0/900K	658,153 [...]]sec ⓘ	Now
1	PRDC	Server Status A		5 minutes	0		N/A - N/A	37	Now
1	PRDC	Server Status B		5 minutes	0		N/A - N/A	27	Now
1	PRDC	Server Status C		5 minutes	0		N/A - N/A	0	Now

Cet affichage n'affiche pas tous les modules des instances car il serait impossible dans le cas de grands environnements. Un nombre configurable de modules est extrait de chaque Instance. Par défaut : 100. Ce paramètre est *Éléments de la Métaconsole* dans la section Gestion des styles visuels. Ce que vous pouvez modifier, en tenant compte du fait que le rendement de la Métaconsole pourrait diminuer si le nombre est très élevé.

Vue des champs personnalisés

Cette vue affiche simplement l'état des agents en fonction de leurs champs personnalisés.

La vue des champs personnalisés se compose de :

- Formulaire de recherche
- Gestion des filtres personnalisés.
- Comptes d'agents et de modules pour chaque valeur du champ personnalisé sélectionné.
- Comptes généraux des agents et des modules.
- Liste des agents filtrés par la recherche.

The screenshot displays the PandoraFMS interface. On the left, there are two sections: 'Antenna' and 'Central'. Each section shows 'Agents by status' and 'Monitors by status' with colored icons representing different states. The 'Antenna' section shows 121 agents and 2192 monitors, while the 'Central' section shows 132 agents and 2396 monitors. On the right, there is a 'Total counters' section with two rows of colored bars representing 'Total Agents' (940, 309, 0, 0, 0) and 'Total Modules' (1,069, 403, 21,128, 0, 0). Below this is a search bar and a table of agents. The table has columns for 'dispositivo', 'Agent', 'I.P', 'Server', and 'Status'. The first four rows of the table are:

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

Formulaire de recherche :

- Group : Il permet de filtrer par groupe.
- Custom fields : Il est obligatoire de sélectionner un champ personnalisé de l'agent. Pour que ce champ puisse être sélectionné, il doit avoir été préalablement créé avec l'option Display up front cochée sur le nœud dans la [section](#) suivante.
- Custom fields Data : Valeur(s) du champ personnalisé.
- Status agents : État(s) de l'agent.
- Module search : Nom du module.
- Status module : État(s) du module.

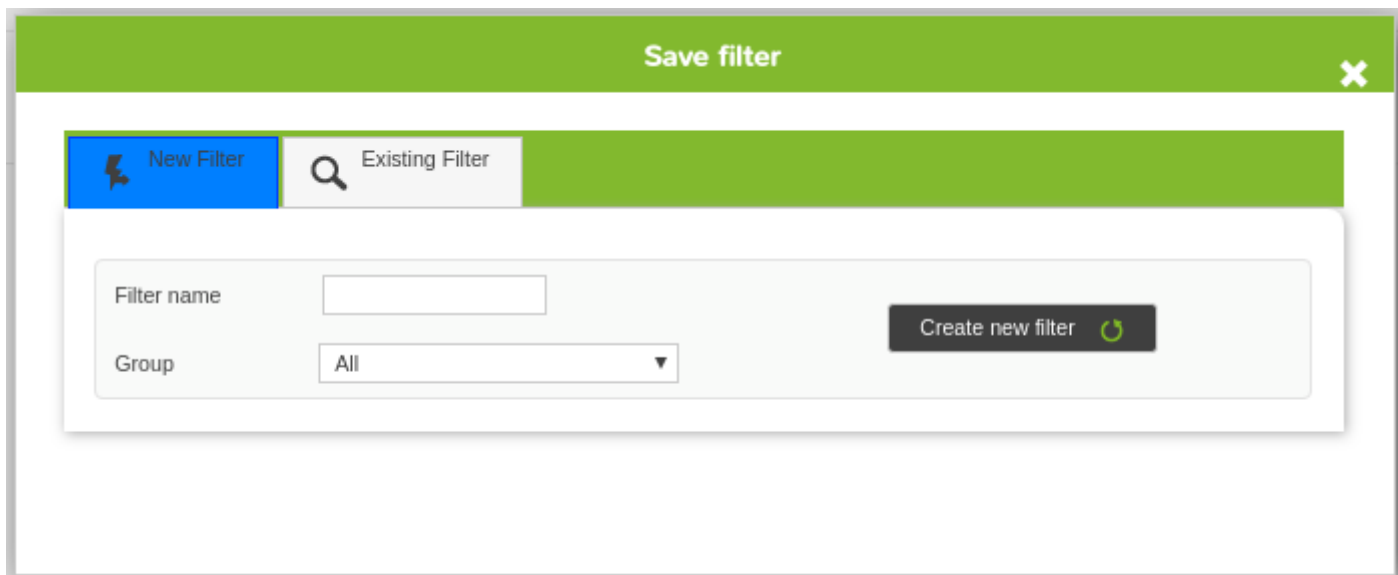
The screenshot shows the search filter configuration form. It includes a 'Show Options' button at the top left. The form is divided into several sections:

- Group:** A dropdown menu set to 'All'.
- Recursion:** A checkbox that is currently unchecked.
- Custom Fields:** A dropdown menu set to 'PandoraFMS'.
- Module search:** An empty text input field.
- Custom Fields Data:** A list box containing the following entries: 'All', '[uri=PandoraFMS.com]Web PandoraFMS[/uri]', '[uri=www.pandorafms.com]ENLACE[/uri]', and '[uri]PandoraFMS.com[/uri]'. A search icon is visible to the right of the list box.
- Status agents:** A list box containing the following entries: 'All', 'Critical', 'Normal', 'Not initialised', 'Not normal', 'Unknown', and 'Warning'.
- Status module:** A list box containing the following entries: 'All', 'Critical', 'Normal', 'Not initialised', 'Not normal', 'Unknown', and 'Warning'.

At the bottom right of the form, there are two buttons: 'Show' with a magnifying glass icon and 'Export to CSV' with a right-pointing arrow icon.

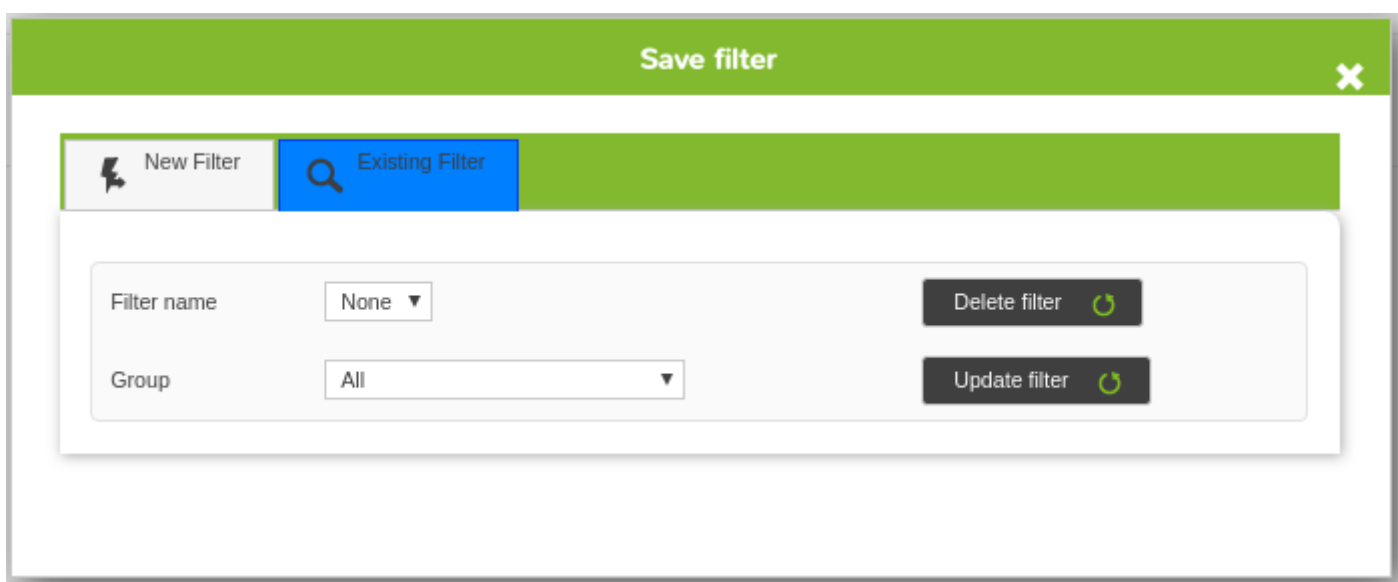
Gestion des filtres personnalisés :

- Créer, mettre à jour et supprimer des filtres : Pour améliorer l'accès à l'affichage des champs personnalisés, vous pouvez créer, enregistrer et supprimer des filtres de recherche. Pour ce faire, les paramètres de recherche sont choisis et il faut cliquer sur l'icône de la disquette. Une fenêtre modale apparaît :
- Nouveau filtre : Utilisé pour la création. Il est obligatoire d'entrer un nom qui n'a pas été utilisé auparavant.



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" (a text box) and "Group" (a dropdown menu currently set to "All"). To the right of these fields is a button labeled "Create new filter" with a green circular refresh icon.

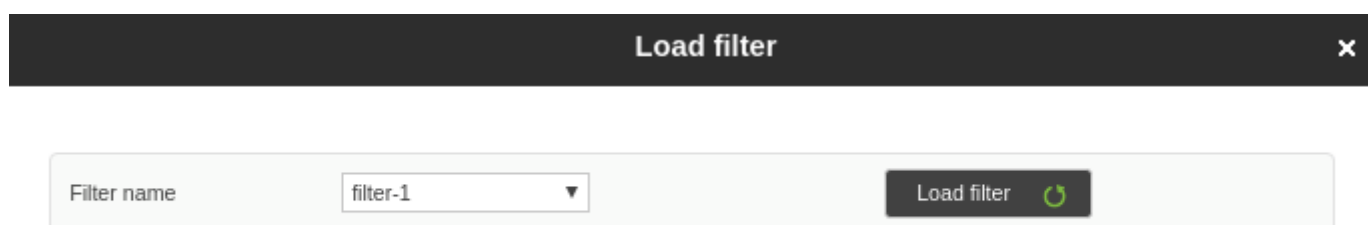
- Filtre existant : Utilisé pour la mise à jour et la suppression.



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

Cette section de gestion des filtres ne sera visible que par les utilisateurs administrateurs.

- Charger les filtres : Cliquez sur l'icône de la flèche et sélectionnez le filtre souhaité.



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 currently set to "filter-1"). To the right of this field is a button labeled "Load filter" with a green circular refresh icon.

- Ajouter des filtres à un utilisateur donné : l'affectation de filtres à des utilisateurs se fait en mode

Création/Modification d'utilisateurs. Lorsque l'utilisateur accède à cette vue, il le fait avec le filtre sélectionné chargé:

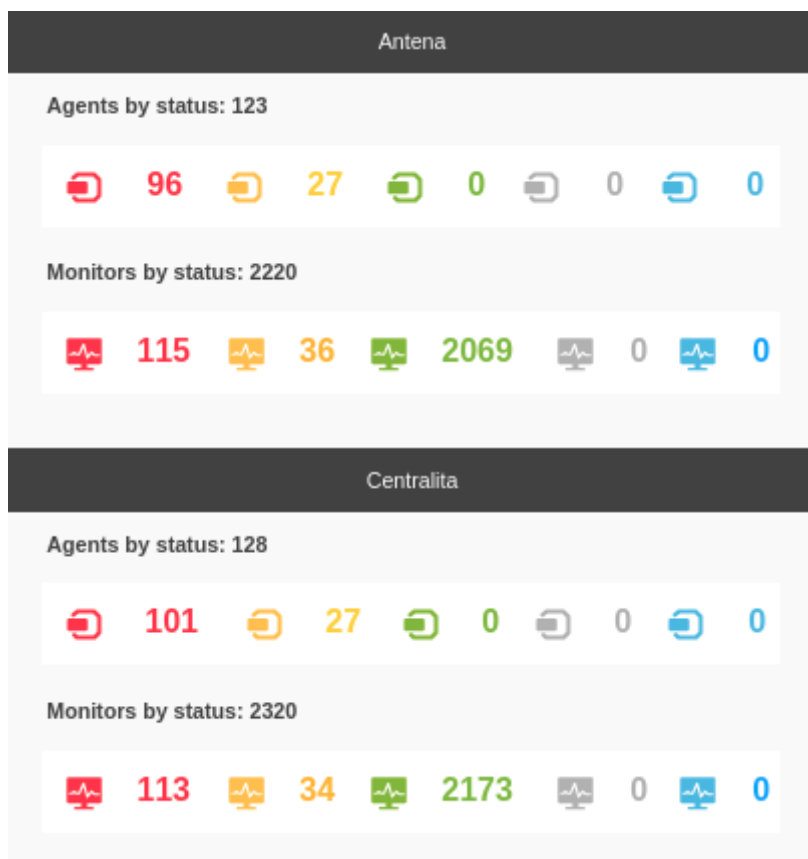
The screenshot shows the 'Create user' form in Pandorafms. The form is divided into several sections:

- User ID:** Includes a user icon, fields for 'Full (display) name', 'Password', and 'Password confirmation', and an 'Administrator user' checkbox.
- Extra info:** Includes fields for 'E-mail' and 'Phone number', and checkboxes for 'Login error', 'Local user', and a 'Session time' field.
- Language:** A dropdown menu set to 'Default'.
- Metaconsole access:** A dropdown menu set to 'Basic'.
- Home screen:** A dropdown menu set to 'Default'.
- Default event filter:** A dropdown menu set to 'test4', highlighted with a red box.
- Timezone:** A dropdown menu set to 'None'.
- Search custom field view:** A dropdown menu set to 'None'.
- Enable agent management:** A checkbox.
- Enable node access:** A checkbox.

At the bottom, there is a 'Comments' section.

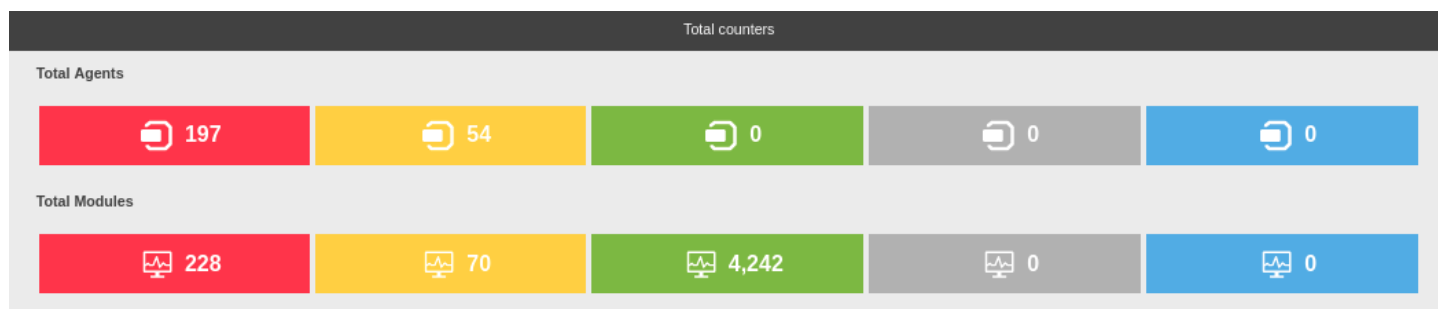
- Comptes d'agents et de modules pour chaque valeur du champ personnalisé sélectionné :

Dans cette section de la vue, vous pourrez visualiser de manière simple les comptes des agents et des modules pour chaque donnée du champ personnalisé sélectionné.



Comptes généraux des agents et des modules :

Dans cette section de la vue, vous pourrez visualiser les comptes des agents et des modules de tous les données des champs personnalisés.



Liste des agents :

Il affiche une liste avec les informations suivantes sur les agents :

- Liste déroulante où les données suivantes de l'agent avec le champ personnalisé choisi seront affichées :
 - Nom du module.
 - Dernière donnée.
 - Seuils.
 - Temps d'intervalle.
 - Dernier temps de contact.
 - État du module.
- Valeur du champ personnalisé.

- Nom de l'agent.
- Adresse IP.
- Serveur.
- État.

Cette table est paginée et peut être recherchée et triée dans les champs par :

- Champ personnalisé.
- Agent.
- Adresse IP.
- Serveur.

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	●

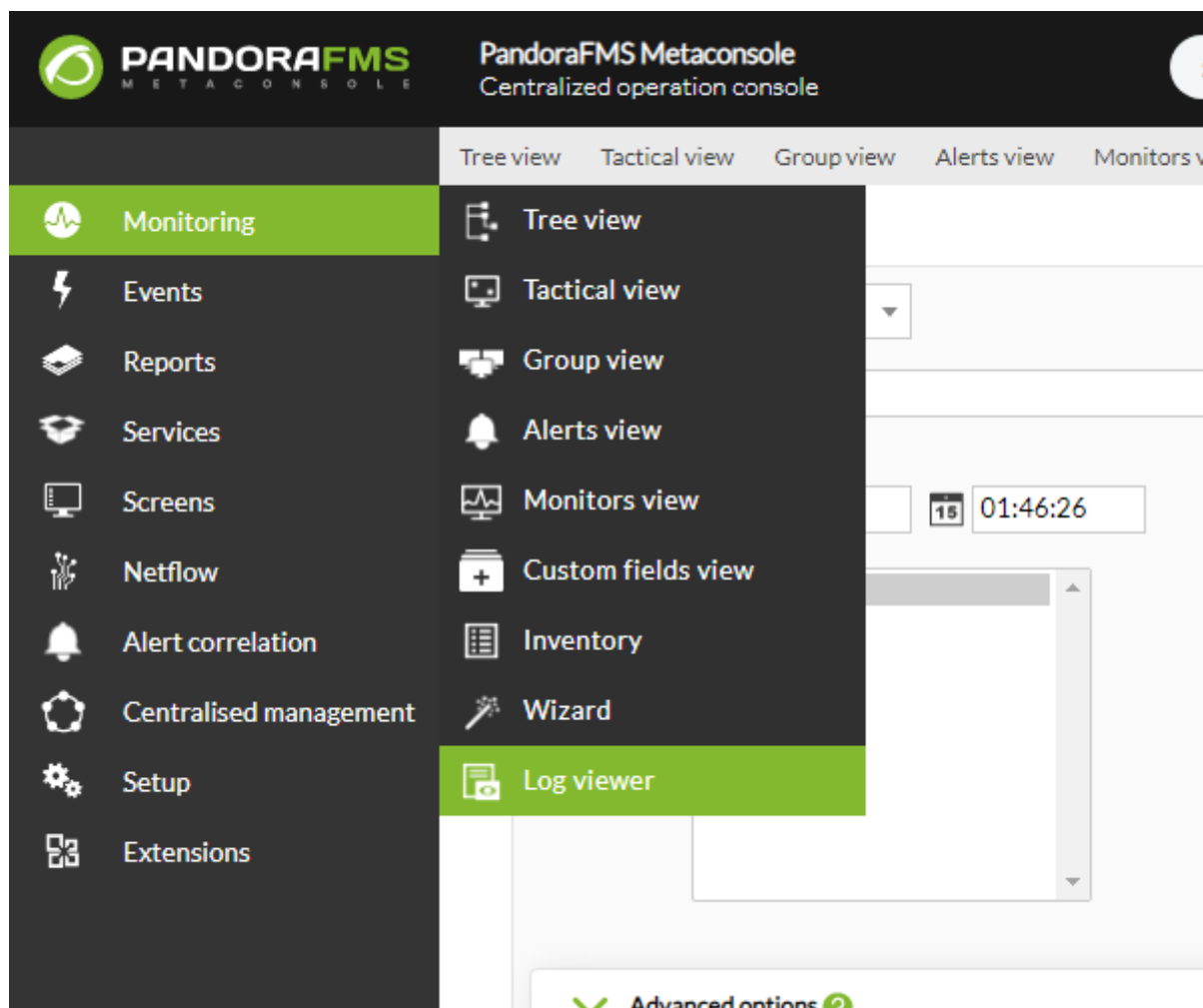
dispositive	Agent	I.P	Server	Status
Central	stress_garrosch_263	127.0.0.1	garrosch	■

Central	stress_varian_751	127.0.0.1	varian	■
Central	stress_garrosch_209	127.0.0.1	garrosch	■
Central	stress_garrosch_308	127.0.0.1	garrosch	■
Central	stress_garrosch_236	127.0.0.1	garrosch	■
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_garrosch_681	127.0.0.1	garrosch	■
Central	stress_varian_1143	127.0.0.1	varian	■
Central	stress_varian_3	127.0.0.1	varian	■
Central	stress_garrosch_691	127.0.0.1	garrosch	■
Central	stress_varian_256	127.0.0.1	varian	■

Showing 1 to 15 of 236 entries

Log viewer

Version NG 747 ou ultérieure.



Vous pouvez trouver le visualiseur de logs dans la section de supervision du menu supérieur. La vue sera similaire à celle trouvée sur les nœuds, mais comprendra un sélecteur multiple supplémentaire pour sélectionner les journaux collectés par des nœuds spécifiques. Dans le [lien](#), vous pouvez voir la description complète des paramètres relatifs à cette vue dans le nœud et qui sont conservés dans la Métaconsole.

Pour accéder à cette vue, vous devez d'abord l'activer dans [les paramètres généraux de la console](#) et configurer la connexion au serveur Elasticsearch, comme décrit dans la section de [configuration du Log Viewer](#).

Ensuite, vous pouvez accéder depuis le menu Monitoring → Log viewer, et vous pouvez sélectionner le filtrage (Start date) de la dernière heure, des 8 dernières heures, etc. ou sélectionner les dates par plage de dates (Select dates by range) :



Search mode: Order:

Search: Group:

Select dates by range:

Start date:

Server: [Advanced options ?](#)

Search mode: Order:

Search: Group:

Select dates by range:

Start date: End date:

Server: [Advanced options ?](#)

Événements

Pandora FMS utilise un système d'événements pour montrer ce qui s'est passé de plus pertinent dans les systèmes surveillés. Dans un lecteur d'événements, il est reflété lorsqu'un moniteur est tombé en panne, qu'une alerte a été déclenchée ou lorsque le système Pandora FMS lui-même a un certain problème.

La Métaconsole possède son propre observateur d'événements où les événements des instances associées sont centralisés. Il est possible de centraliser les événements pour toutes les instances ou seulement une partie d'entre elles. Lorsque les événements d'une instance sont répliqués sur la Métaconsole, leur gestion devient centralisée dans la Métaconsole, de sorte que leur affichage dans l'instance sera limité à la lecture seule.

La réplification d'événements des instances vers la Métaconsole

Afin que les instances répliquent leurs événements vers la Métaconsole, il sera nécessaire de les configurer individuellement.

Plus d'informations de leur configuration dans la section [Installer et configurer la Métaconsole](#) du

manuel

Gestion d'événements

La gestion d'événements pour leur visualisation se divise dans la vue et sa configuration.

Voir événements

Vue des événements

La vue normale des événements, les événements non validés datant de moins de 8 heures, est accessible en cliquant sur l'icône Événements de la page principale de la Métaconsole.

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

La création et la modification des filtres d'événements fonctionnent de la même manière que ceux des nœuds. Les valeurs par défaut du filtre de la vue des événements sont les suivantes :



Filter

Group

Event type

Event status

Max. hours old

Duplicate

Free search

Severity
Critical
Critical/Normal

Group recursion

Search in secondary groups

Advanced options


La seule différence avec les filtres d'événements sur les nœuds est le champ Server qui vous permet de choisir la Métaconsole et/ou un ou plusieurs nœuds.

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

<ul style="list-style-type: none">configurationcpu_usagecriticaldisk_ratedisk_usagedmzdmz testmemory_usagnetworknetwork_usag	<input type="text" value="None"/>
---	-----------------------------------

Events without the following tags

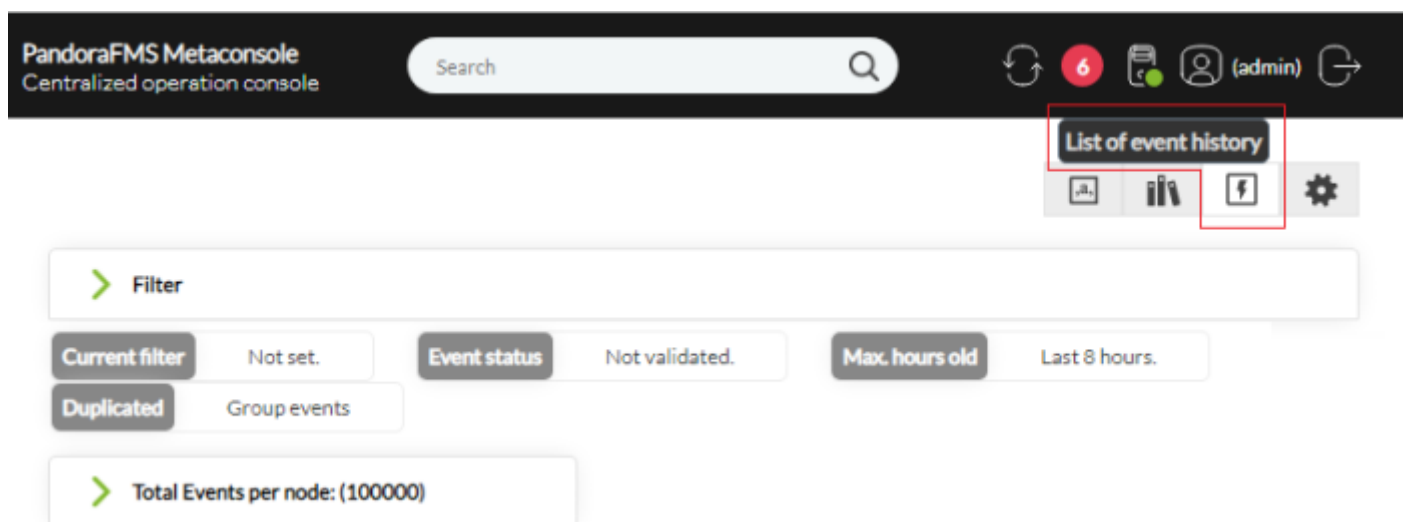
<ul style="list-style-type: none">configurationcpu_usagecriticaldisk_ratedisk_usagedmzdmz testmemory_usagnetworknetwork_usag	<input type="text" value="None"/>
---	-----------------------------------

Lors de la mise à niveau vers la version 767, il se peut que les filtres précédemment créés *ne soient pas configurés dans la section Serveur* (Server). Si tel est le cas, reconfigurez vos préférences de serveur pour chaque filtre et enregistrez à nouveau pour corriger le problème.

Historique des événements

Pour avoir un historique des événements, vous devez activer et configurer cette option dans ►Setup → Metasetup → Performance et ainsi les événements plus anciens d'un certain temps (configurable), qui n'ont pas été validés, passeront automatiquement à une vue secondaire : Vue de l'historique des événements.

Cette vue est identique à la vue d'événements normaux et est accessible à partir d'un onglet dans la vue d'événements.

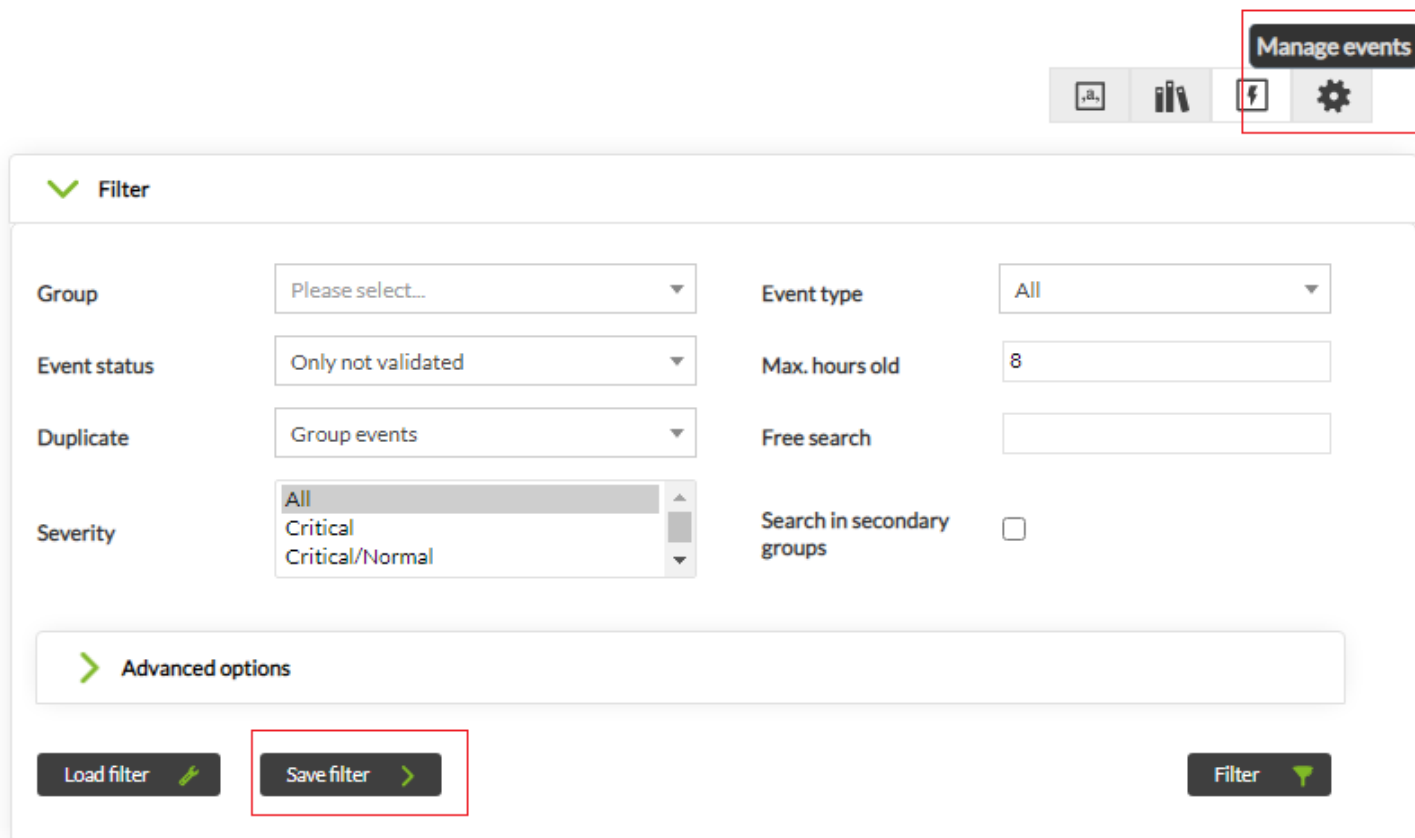


The screenshot displays the PandoraFMS Metaconsole interface. At the top, there is a dark header with the text 'PandoraFMS Metaconsole Centralized operation console' on the left, a search bar in the center, and several icons on the right including a refresh button, a notification bell with '6', a calendar, a user profile labeled '(admin)', and a share icon. Below the header, a navigation bar contains several icons, with the 'List of event history' tab highlighted in a red box. Below the navigation bar, there is a filter section with a 'Filter' button and several filter options: '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 summary box showing 'Total Events per node: (100000)'.

Filtre d'événements

Les vues d'événements disposent d'une série d'options de filtrage pour adapter la vue aux besoins de l'utilisateur.

Vous pouvez créer des options de filtrage de deux manières différentes. L'une d'elles consiste à effectuer le filtrage dans la même visualisation des événements, en vous donnant pour enregistrer le filtrage sélectionné dans le bouton ►Save filter.



The image shows a screenshot of the Pandora FMS interface. At the top right, there is a navigation bar with several icons, including a gear icon labeled "Manage events" which is highlighted with a red box. Below this is a "Filter" section with a green checkmark icon and the word "Filter". The filter section contains several fields:

- Group:** A dropdown menu with "Please select..." as the selected option.
- Event status:** A dropdown menu with "Only not validated" as the selected option.
- Duplicate:** A dropdown menu with "Group events" as the selected option.
- Severity:** A dropdown menu with "All" as the selected option. The dropdown list is open, showing "All", "Critical", and "Critical/Normal".
- Event type:** A dropdown menu with "All" as the selected option.
- Max. hours old:** A text input field containing the number "8".
- Free search:** An empty text input field.
- Search in secondary groups:** A checkbox that is currently unchecked.

Below the filter fields is a section labeled "Advanced options" with a green arrow icon. 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 (highlighted with a red box), and "Filter" with a green arrow icon.

D'autre part, en cliquant sur l'icône Manage Events → Filter List → Create new filter et créer manuellement les différents filtres possibles dont vous avez besoin. Vous pourrez ensuite charger les filtres créés dans les options de filtrage des événements.



Create Filter

Filter name

Save in group i

Group

Event type

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

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 >

Détails d'un événement


Dans les listes d'événements (normal ou historique), vous pouvez voir les détails d'un événement en cliquant sur le nom de l'événement ou sur l'icône « Afficher plus » du champ d'action.


Custom data	Timestamp	Event name	Agent ID	Status	Agent name	Event Id	Options	
	Now	Module 'Connections opened' is going to WARNING (421)	106	★	koldo. 32	3400 9448	   	<input type="checkbox"/>
	Now	Module 'Connections opened' is going to WARNING (412)	113	★	koldo. 39	3400 9454	   	<input type="checkbox"/>
	Now	Module 'Connections opened' is going to CRITICAL (464)	107	★	koldo. 33	3400 9449	   	<input type="checkbox"/>
	Now	Module 'Connections opened' is going to WARNING (405)	109	★	koldo. 35	3400 9452	   	<input type="checkbox"/>


Les champs d'un événement apparaissent dans une nouvelle fenêtre avec plusieurs onglets


Général


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

Le premier onglet affiche les champs suivants :

- Event ID : C'est un identifiant unique pour chaque événement.
- Nom de l'événement : C'est le nom de l'événement qui comprend une description de celui-ci.
- Date et heure : Date et heure auxquelles l'événement est créé dans la console d'événements.
- Propriétaire : Nom de l'utilisateur propriétaire de l'événement.
- Type : Type d'événement. Il peut y avoir les types suivants : Alerte terminée, Alerte déclenchée, Alerte récupérée, Modification des paramètres, Inconnu, Équipement réseau reconnu par le Recon, Erreur, Moniteur en état critique, Moniteur en état Warning, Moniteur en état Unknown, Non normal, Système et Validation manuelle d'une alerte.
- Répété : Il définit si l'événement est répété ou non.
- Priorité : Il affiche la priorité de l'événement. Il existe les niveaux suivants : Maintenance, Information, Normal, Mineur, Avertissement, Major et Critique.
- État : Il affiche l'état dans lequel se trouve l'événement. Il existe les états suivants : Nouveau, validé et en cours.
- Validé par : Dans le cas où l'événement a été validé, il montre l'utilisateur qui l'a validé, la date et l'heure où il l'a fait.
- Groupe : Dans le cas où l'événement provient d'un module d'agent, il affiche le groupe auquel appartient l'agent.
- Étiquettes : Dans le cas où l'événement provient d'un module d'agent, il affiche les étiquettes du module.
- Extra ID : Identifiant supplémentaire qui est placé sur l'événement pour pouvoir le rechercher en tant que texte libre.

Détails

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


Le deuxième onglet affiche les détails de l'agent et du module qui a généré l'événement. Vous pouvez même accéder au graphique du module.


La dernière donnée est l'origine de l'événement qui peut être un serveur Pandora FMS ou n'importe quelle source lorsque l'API est utilisée pour générer l'événement.


Champs d'agent


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


Le troisième onglet affiche les champs personnalisés de l'Agent.


Commentaires


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.

Le quatrième onglet affiche les commentaires qui ont été ajoutés à l'événement et les changements qui se sont produits, tels que le changement de propriétaire ou la validation de l'événement.

Réponses

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			

Le cinquième onglet affiche les actions ou les réponses qui peuvent être effectuées sur l'événement. Les actions à entreprendre sont les suivantes :

- Changer le propriétaire.
- Changer l'état.
- Ajouter un commentaire.
- Supprimer l'événement.
- Exécuter une réponse personnalisée : toutes les actions configurées par l'utilisateur peuvent être exécutées.

Configurer les événements

Les utilisateurs avec le bit ACLs EW auront un onglet disponible pour accéder au panneau de configuration des événements.

PandoraFMS Metaconsole
Centralized operation console

Search

6

(admin)

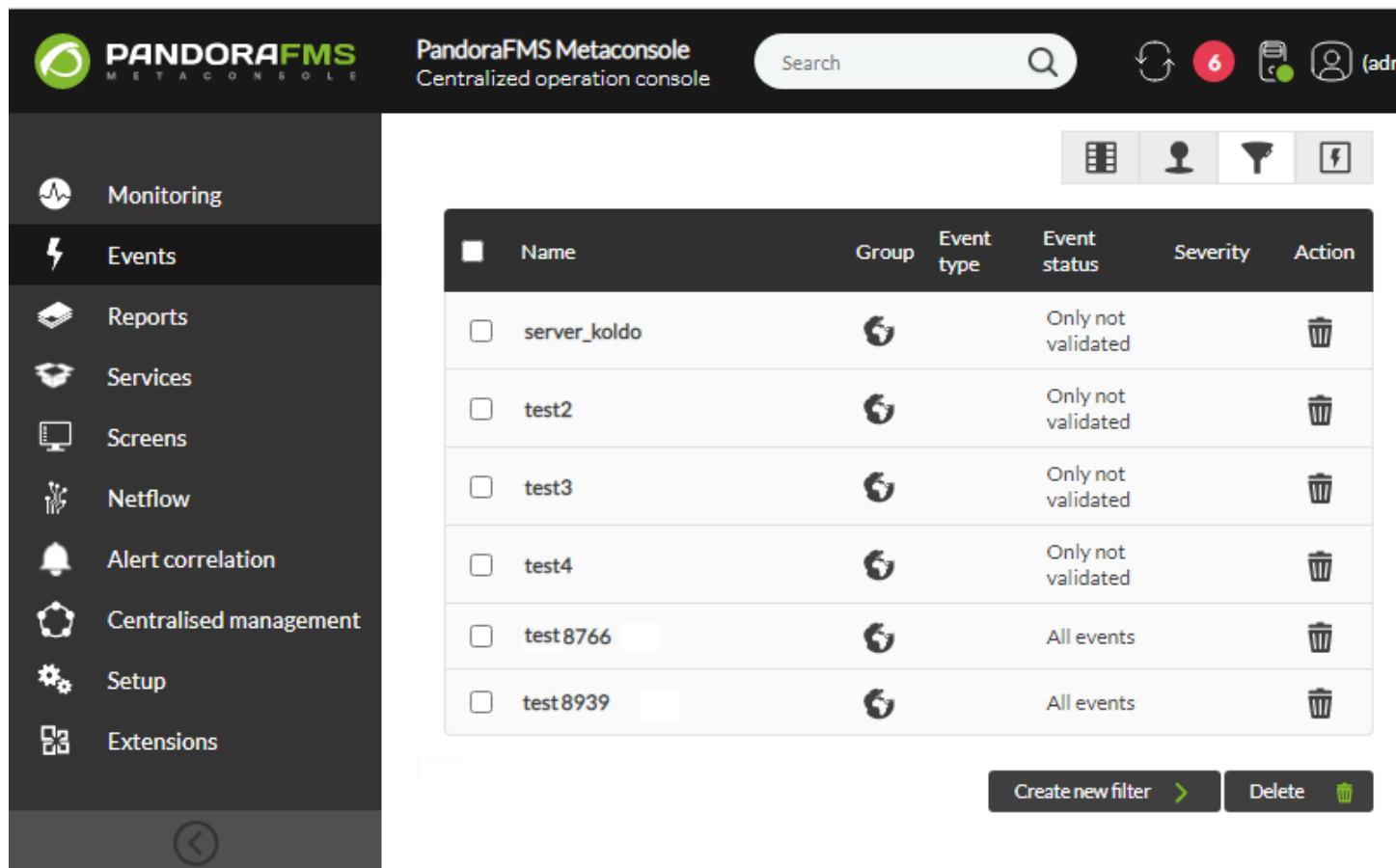
Manage events

Gérer les filtres d'événements

Les filtres d'événements permettent de paramétrer les événements à afficher dans la console d'événements. Avec Pandora FMS, vous pouvez créer des filtres prédéfinis à utiliser par un ou

plusieurs utilisateurs.

Les filtres peuvent être modifiés en cliquant sur le nom du filtre.



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. 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		

Pour créer un nouveau filtre, cliquez sur le bouton "Créer des filtres". Une fois là, une page apparaît où les valeurs du filtre sont configurées.



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 ➤

Les champs que vous pouvez filtrer sont les suivants :

- Group : Combo où vous pouvez choisir le groupe Pandora FMS.
- Event Type : Combo où vous pouvez choisir le type d'événement.
- Severity : Combo où vous pouvez choisir en fonction de la gravité de l'événement.
- Event Status : Combo où vous pouvez choisir en fonction de l'état de l'événement.
- Free search : Champ qui permet une recherche libre d'un texte.
- Agent Search : Combo où vous pouvez choisir l'agent source de l'événement.
- Max hour old : Champ où les heures sont affichées.
- User Ack : Combo où vous pouvez choisir parmi les utilisateurs qui ont validé un événement.
- Repeated : Combo où vous pouvez choisir entre afficher les événements répétés ou afficher tous les événements.

En plus des champs de recherche dans le menu Event Control filter, l'option Block size for pagination apparaît, où vous pouvez choisir parmi le nombre d'événements qu'il y aura sur chaque page au moment de la pagination.

Gérer les réponses

Dans les événements, vous pouvez configurer des réponses ou des actions à effectuer sur un événement donné. Par exemple, faire un *ping* à l'IP de l'agent qui a généré l'événement, se connecter par SSH à cet agent, etc.

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 a menu with options: Monitoring, Events (selected), Reports, Services, Screens, Netflow, Alert correlation, Centralised management, Setup, and Extensions. The main content area displays a table of responses with the following columns: Name, Description, Group, and Actions. The table contains six rows of data. Below the table is a 'Create response' button with a right-pointing arrow.





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	🌐	🗑️ ✎️

[Create response >](#)

La configuration des réponses permet de configurer à la fois une commande et une URL.

Pour ce faire, vous pouvez définir une liste de paramètres séparés par des virgules qui seront remplis par l'utilisateur lors de l'exécution de la réponse. Vous pouvez également utiliser les macros internes de l'événement et celles de cette liste :

- Adresse de l'agent : `_agent_address_`
- ID de l'agent : `_agent_id_`
- ID de l'alerte associée à l'événement : `_alert_id_`
- Date à laquelle l'événement s'est produit : `_event_date_`
- Id extra : `_event_extra_id_`
- Id de l'événement : `_event_id_`
- Instructions de l'événement : `_event_instruction_`
- Id de criticité de l'événement : `_event_severity_id_`
- Criticité de l'événement (traduit par la console de Pandora FMS) : `_event_severity_text_`
- Origine de l'événement : `_event_source_`
- État de l'événement (Nouveau, validé ou événement en cours) : `_event_status_`
- Étiquettes d'événement séparées par des virgules : `_event_tags_`
- Texte intégral de l'événement : `_event_text_`
- Type d'événement (Système, Changement d'état inconnu...) : `_event_type_`
- Date à laquelle l'événement s'est produit au format utimestamp : `_event_utimestamp_`
- ID du groupe : `_group_id_`
- Nom du groupe dans la base de données : `_group_name_`
- Adresse du module associé à l'événement : `_module_address_`
- ID du module associé à l'événement : `_module_id_`
- Nombre du module associé à l'événement : `_module_address_`
- Utilisateur propriétaire de l'événement : `_owner_user_`
- ID de l'utilisateur : `_user_id_`
- Identifiant de l'utilisateur qui lance la réponse : `_current_user_`
- Champs personnalisés : Les champs personnalisés de l'événement sont également disponibles dans les macros de réponse aux événements. Ils auraient la forme de `_customdata__CKG_*` où il faudrait remplacer l'astérisque (*) par la clé du champ personnalisé à utiliser.
 - `_customdata_X_` : Il sorte un champ spécifique de *custom_data*, en remplaçant le X par le nom du champ.
 - `_customdata_json_` : Il sorte les informations de *custom data* au format JSON.
 - `_customdata_text_` : Il sorte toutes les informations de *custom data* en mode texte.

Edit event responses


Name	<input type="text"/>	Group	<input type="text" value="All"/>
Description	<div style="border: 1px solid #ccc; height: 80px;"></div>		
Location (i)	<input type="text" value="Modal window"/>	Size	Width (px) <input type="text" value="620"/> Height (px) <input type="text" value="500"/>
Parameters	<input type="text"/>	Type	<input type="text" value="Command"/>
Command (?)	<div style="border: 1px solid #ccc; height: 80px;"></div>		
Display command (i)	<input type="checkbox"/>		

Create >

Personnaliser les champs de la vue des événements

Avec Pandora FMS, il est possible d'ajouter ou de supprimer des colonnes dans la vue des événements, chaque colonne est un champ d'informations sur l'événement, il est donc possible de personnaliser cette vue.

The screenshot displays the PandoraFMS Metaconsole interface. The top navigation bar includes the PandoraFMS logo, the text 'PandoraFMS Metaconsole Centralized operation console', and a search bar. A sidebar on the left contains menu items: 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 search bar, a list of 'Fields available' (Agent IP, User, Group, Event Type, Module Name, Alert, Severity, Comment, Tags, Source), and a list of 'Fields selected' (Custom data, Severity mini, Timestamp, Event name, Agent ID, Status, Agent name, Event Id). A 'Update' button is located at the bottom right of the field selection area.

- À partir de cet écran, vous pouvez ajouter des champs dans la vue des événements en passant de la case de droite, Champs disponibles (Fields available), à la case de gauche, Champs sélectionnés (Fields selected), à l'aide de la flèche horizontale.
- Pour supprimer des champs de la vue des événements, il faut les déplacer de la case de droite à la case de gauche à l'aide de la flèche horizontale.
- Vous pouvez également modifier l'ordre des champs dans le Field selected en les sélectionnant un par un et en cliquant sur les flèches verticales situées sous la liste.
- Pour restaurer les champs avant la modification, cliquez sur l'icône  .

Rapports

Dans la Métaconsole, vous pouvez faire toutes sortes de rapports sur les données des instances. La configuration d'un rapport est stockée dans la Métaconsole, mais lorsqu'elle est affichée, elle obtient les données en se connectant aux instances.

Pour l'éditeur de rapports, la provenance des agents et des moniteurs est transparente. L'utilisateur ne saura pas de quelle instance ils proviennent.

Vous pouvez créer des rapports de deux manières :

- Manuellement
- Avec des modèles de rapports

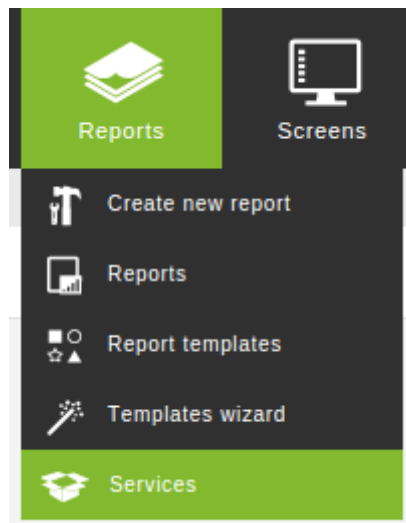
Pour en savoir plus, consultez la section [Rapports](#) de documentation.

Supervision des services sur la Métaconsole

Comme nous l'avons vu dans la section de supervision des services sur les nœuds, un service est un regroupement de ressources informatiques en fonction de leurs fonctionnalités.

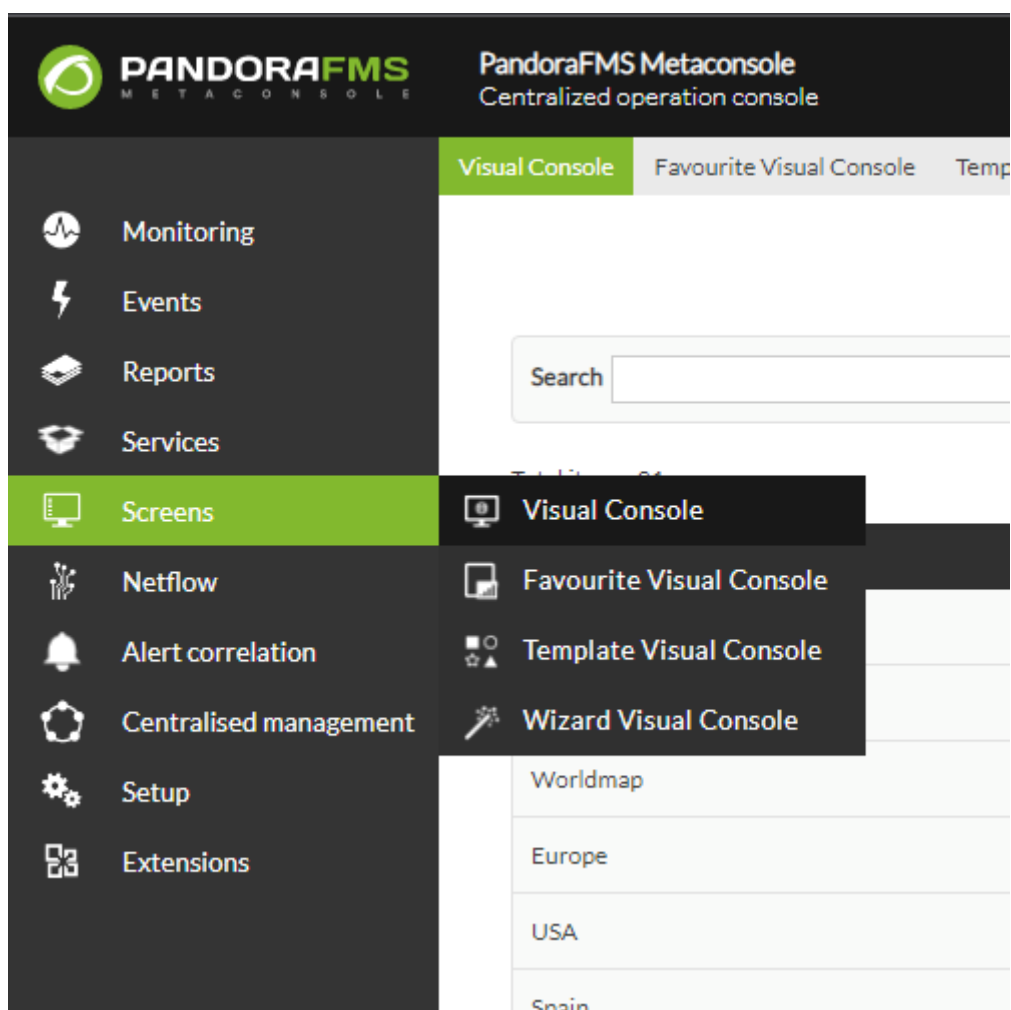
Avec la supervision des services sur la Métaconsole, vous pouvez regrouper les services présents sur les nœuds et vérifier d'un simple coup d'œil l'état global des ressources.

Dans la Métaconsole, vous pouvez les ajouter comme suit : - Sélectionnez l'option "Rapports" → "Services"



Pour en savoir plus sur la création et la configuration des services, consultez la section Services de ce [lien](#).

Écrans

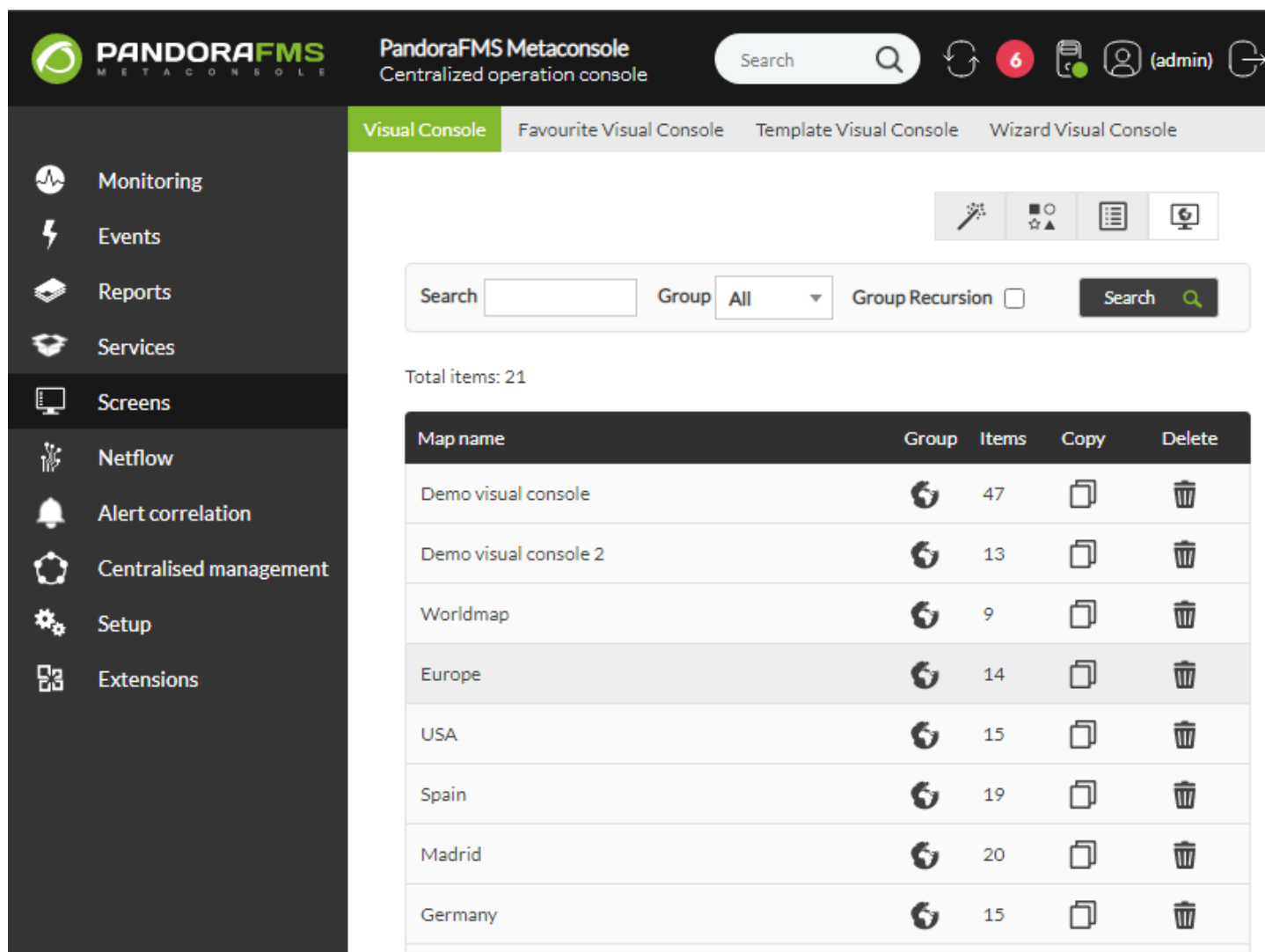


Pour activer ces menus, reportez-vous aux [paramètres généraux de la Metaconsole](#).

Console visuelle

Dans la Métaconsole, vous pouvez configurer une console visuelle, qui est un panneau composé d'un arrière-plan et d'éléments placés dessus.

La configuration et la présentation des données sont exactement les mêmes que sur les cartes visuelles de la console normale, sauf que les données sont obtenues à partir des instances de manière transparente pour l'utilisateur.



The screenshot displays the PandoraFMS Metaconsole interface. The top header includes the PandoraFMS logo, the title "PandoraFMS Metaconsole Centralized operation console", a search bar, a refresh button, a notification badge with the number 6, a user profile icon for "admin", and a navigation arrow. Below the header, a navigation bar highlights "Visual Console" and lists other options: "Favourite Visual Console", "Template Visual Console", and "Wizard Visual Console". On the left, a dark sidebar menu contains icons and labels for: Monitoring, Events, Reports, Services, Screens, Netflow, Alert correlation, Centralised management, Setup, and Extensions. The main content area features a search bar, a "Group" dropdown menu set to "All", a "Group Recursion" checkbox, and a search button. Below this, it indicates "Total items: 21". A table lists the visual console maps with columns for Map name, Group, Items, Copy, and Delete.

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		

Toutes ces informations sont rassemblées dans la section [Cartes visuelles de Pandora FMS](#) des nœuds.

NetFlow

The screenshot shows the PandoraFMS Metaconsole interface. The top navigation bar includes the PandoraFMS logo, the title 'PandoraFMS Metaconsole Centralized operation console', a search bar, and several utility icons. The left sidebar contains a menu with the following items: Monitoring, Events, Reports, Services, Screens, Netflow (highlighted in green), 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' duration selector); 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'.

Pour pouvoir disposer de cette option dans la Métaconsole, vous devez avoir activé l'affichage de la section, dans les [options générales](#) du Metasetup de la Métaconsole. À son tour, pour pouvoir faire le NetFlow d'un nœud à partir de la Métaconsole, le nœud devra également avoir le NetFlow actif dans sa configuration.

Pour en savoir plus sur la façon d'effectuer la Live view et les filtres possibles de NetFlow, ainsi que l'installation des dépendances nécessaires, visitez la section Netflow [sur ce lien](#).

Vous ne pouvez extraire que le flux d'informations d'un nœud, vous ne pouvez pas extraire les informations de plus d'un en même temps.

[Retour à l'index de documentation Pandora FMS](#)