

Monitoring alerts

Alertes de monitoring

- Tous les ordinateurs
- Tous les ordinateurs gpi
- Groupe favoris
- Tous les groupes
- Ajouter un groupe
- Réveil réseau
- Liste des machines non-inventorées
- Alertes de monitoring

Nom machine	Date d'événement	Type d'événement	Message machine	Périphérique	Statut	Message	Numéro de série	Firmware	Commentaire	Actions
<div>ELEMENTS 0 à 0 - Total 0</div>										

This section centralizes all alerts generated by monitored machines in your Medulla environment. It allows you to track, in real time or delayed, hardware or software incidents detected by supervisors deployed on your machines.

Objective

- **Identify critical or recurring incidents** : such as disk failures, device errors, network anomalies, or any other problem affecting monitored machines.
- **Ensure clear traceability of events** : by keeping a precise time stamp for each alert in order to ensure a complete follow-up.
- **Allow rapid reaction** by alerting administrators to detected problems so that they can respond quickly.

Alert history

When no alert is currently active, you can view history of past events. This includes resolved alerts, thus ensuring complete traceability of incidents and interventions on your machines.

Information available in history:

If alerts are recorded, the table will show the following:

- **Name of machine** : Name of the machine concerned by the alert.
- **Date of event** Date and time of incident.
- **Type of event** Category of incident (e.g. device error, hardware failure).
- **Machine message** : Details of the error or problem raised by the machine.
- **Device concerned** : The device related to the incident (e.g. hard drive, network card).
- **Status** Current status of the alert (open, ongoing, resolved).
- **Message** : Alert message generated by the Supervisory Officer.
- **Serial number** : Device or machine serial number.
- **Firmware** : Version of the firmware involved in the incident.
- **Commentary** : Space for comments or clarifications on the incident.
- **Available actions** : Actions to be undertaken on the incident (e.g. solve, ignore, export).

In particular: If the table is empty, this means that no alerts have yet been detected or stored in your environment.

Monitoring Configuration

Tous les ordinateurs	<div>Configuration du monitoring</div> <div>Le fichier sera enregistré automatiquement</div> <div>Editer le fichier /var/lib/pulse2/xmpp_monitoring/confagent/monitoring_config.ini</div> <div></div>
Tous les ordinateurs gipi	
Groupes favoris	
Tous les groupes	
Ajouter un groupe	
Réveil réseau	
Liste des machines non-inventoriées	
Alertes de monitoring	
Configuration du monitoring	

In this section, you can customize the monitoring settings applied to positions via a centralized configuration file.

When you access this page, an edit area is displayed directly on the screen, allowing you to change the contents of the following configuration file

```
/var/lib/pulse2/xmpp_monitoring/confagent/monitoring_config.ini
```

All changes you make in this space are **automatically recorded**, no need to click on a validation button.

Recommendations

Before any modification, it is advisable to make a **backup of existing file**.

Apply the changes with **precautionary** and test them on a few machines.

Contact your system administrator if you have a doubt about a parameter.

Revision #1

Created 12 May 2025 14:15:59 by DocsAdmin

Updated 12 May 2025 14:16:02 by DocsAdmin