Introduction to Monitoring

Introduction to Monitoring

We are working on the translation of the Pandora FMS documentation. Sorry for any inconvenience.

Introduction to Monitoring

Monitoring consists of executing processes on all types of systems to collect and store data, and then carry out actions and make decisions based on the information obtained.

Logical Agents in Pandora FMS

The monitoring carried out by Pandora FMS is classified into Logical Agents, which always belong to a Group. These are equivalent to each of the different computers, devices, websites or applications that are subject to monitoring.

These Agents defined in the Pandora FMS Console can present local data collected through a Software Agent, remote data collected through network checks, or both types of data.

Comparison of monitoring based on Software Agents and Remote Monitoring

- Agent-based monitoring consists of installing a small program (Software Agent) that remains running on the system, obtaining data locally, by executing commands and/or scripts (scripts).
- Remote monitoring consists of using the network to perform remote checks on the systems, without the need to install any additional component on the equipment to be monitored.

Configuring an Agent in the Console

Management menu → Resources → Manage agents, click on the agent name, click on the Management icon.

Main editing interface fields in normal view

- Alias: For the proper functioning of all the functions that Pandora FMS performs through agents and modules, avoid the use of the following characters /, \, |, %, #, & and $ for the name of the agent or module. If these agents contain such characters, they can create confusion with the use of system paths or execution of other commands, causing errors on the server.
- Server: Server that will execute the checks configured in agent monitoring, special parameter in case of having configured HA in your installation.
- Primary group: It allows you to assign a group to the agent. Clicking on the group icon will lead you to the assigned group tactical view.

- IP address: It allows you to assign an IP address to the agent. With the Check unique IP button you may check whether the IP address entered is free, if it is already in the list of saved addresses for that agent (it has a deletion option) or if it is in use by another agent. In case it is used by another agent, when saving the modifications, it will warn about it and it will ask for a confirmation before registering this data. In the General Configuration it could be configured so that the Check unique IP button is automatically used for editing all the agents.

Main editing interface fields in advanced view

- Secondary groups: Optional parameter so that an agent can belong to more than one group (secondary groups).
- Cascade protection services: To prevent a flood of cascading alerts. You may choose an agent or an agent module. In the first case, when the chosen agent is critical, the agent will not generate alerts; in the second case, only when the specified module is critical, the agent will not generate alerts.

Three work modes can be selected for Module definition:

- Learning mode: Default mode, if an XML arrives with new modules, they will be created automatically; it is a learning behavior.
- Normal mode: If an XML arrives with new modules, they will only be created if they were previously declared in the Console.
- Autodisable mode: It is the same as the learning mode, but if all modules go to unknown, the agent will be disabled until new information arrives.

Agent Display

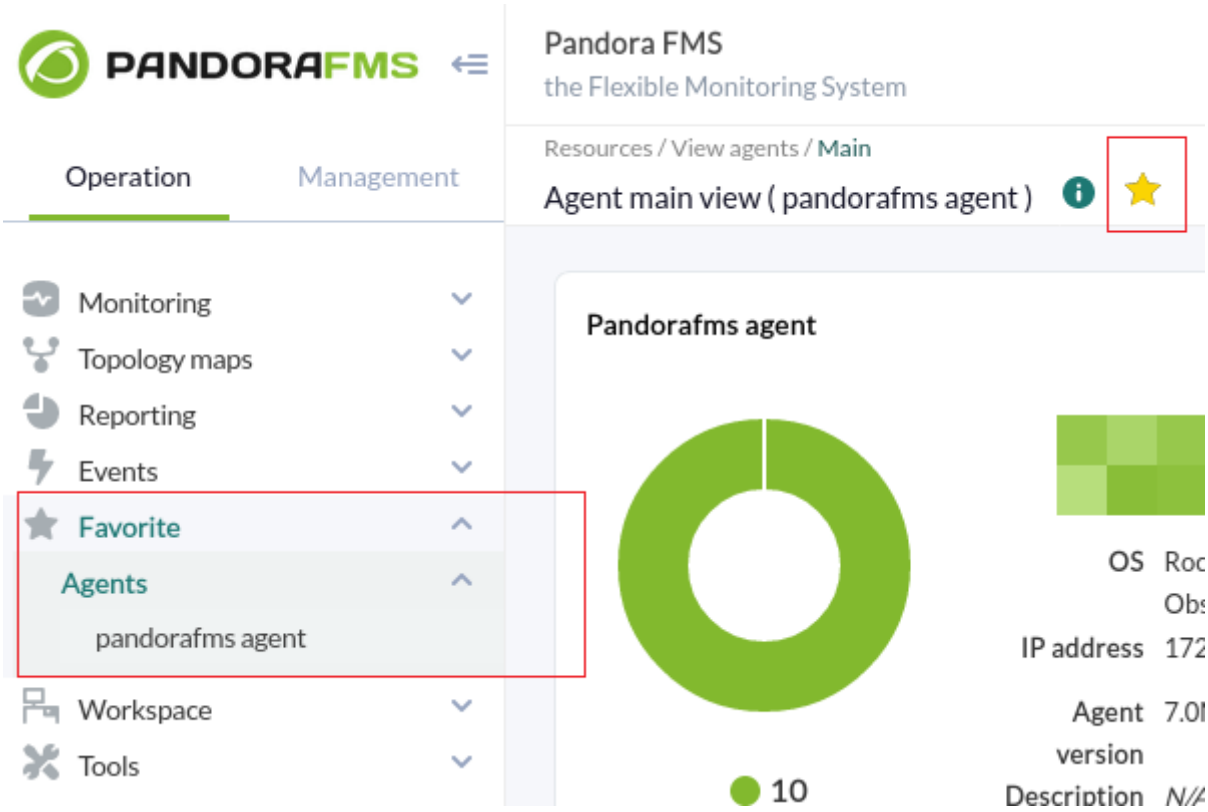
Management menu → Resources → Manage agents, click on the agent name.

This screen offers a large amount of information regarding the agent, with the possibility of forcing the execution of remote checks and refreshing data. At the top it shows a summary with various agent data.

- Total number of modules and their status.
- Events in the last 24 hours.
- Agent information.
    - Name.
    - Version.
    - Agent accessibility.
    - Cluster.
- List of modules: belonging to the agent and their respective states (only initialized modules).
- Full list of alerts from the agent, with the option to select one or more alerts and validate them.
- Status of log sources as configured in Log Collection.
- List with the last events of the agent, with the option to show only the events of the last 24 hours.

Version 770 or later.

Using the favorite system you can add any agent to a custom list for each user. Click the star button right next to the agent's name in your main view.



You can add (or remove) as many agents as you need, all of them will always be visible in the Agents section of the Favorite menu (Operation section).

Modules

Modules are units of information stored within an Agent with which information is extracted from the device or server to which the agent points.

Each Module can store only one type of metric, within an agent each module has a unique name.

Associated State:

- Not started: Waiting for data reception.
- Normal: Receiving data with values that fall outside of warning or critical thresholds.
- Warning: Data within that threshold.
- Critical: Data falling within that threshold.
- Unknown: The module has been running and has stopped receiving information for a certain time.

Modules have one of several data types: boolean, numeric or alphanumeric, among others.

Module types

- Data Module .

- Network Module.
- Plugin module.
- WMI Module.
- Prediction module.
- Webserver module.
- Web analytics module.

Status monitoring

When talking about monitoring, there is the concept of state, which is the association of the "relative value" instead of the absolute value, so that when a threshold is exceeded, the state changes.

Pandora FMS allows you to define thresholds to define the status that a checkup will have based on the data it collects. The three possible states are: `NORMAL`, `WARNING` and `CRITICAL` .

- Warning status: If the numerical value of the module is within the lower and upper limits. If no upper limit is specified, any value higher than the lower limit will cause the state to change.
- Critical: Same as the previous point, only for the `critical` state.
- Inverse interval: Present for both the `warning` and `critical` thresholds, if enabled, the module will change state when its values get outside the specified interval. It also works for alphanumeric modules.
- Percentage: If enabled, the threshold value is interpreted as a percentage. The way Percentage thresholds work is by comparing the new value reported by the module regarding the previous one, to see the variation percentage, and if it complies with the increase (Max.) or decrease (Min.) percentage limits established, it will change state or not.

If the warning and critical thresholds overlap at any range,
the critical threshold will always prevail.

Basic Options

It must always be kept in mind that this interface is used both by local monitoring as well as by remote monitoring and parameters that are valid in one or another area are presented. For example, the parameters Timeout and Retries (Retries) are useless in local monitoring (local checks) but are important in remote monitoring.

- Using module component: When using a module component they will be automatically filled with parameter values necessary to perform the monitoring, this token appears in all types of modules, except in those of prediction.
- Module group: Allows you to assign the module to a defined module group.
- Type: Type of module depending on the type of data returned. By selecting Using module component the data type will be chosen automatically.
- Change to critical status after X intervals in warning status: (version 766 or later) This token allows

you to promote a module's status change to critical if it has been X times in a row (continuous monitoring intervals) in warning state.
    - For example, if a value of 2 is placed: **warning → warning → warning → CRITICAL**.
    - Important: This token works in conjunction with FF threshold, for example Change to critical... to 1 and FF threshold to 1 :
        - **normal → normal → warning → warning → CRITICAL**.
- Historical data: Check this option if you need to save long-term values in the databasehistorical cough.
- Target IP and Port: IP address and port number to which to query to obtain monitoring values. In some cases, such as with WMI monitoring, additional text fields will appear to set connection credentials and even query strings.

Advanced Options

You should always bear in mind that this interface is used by both local monitoring as well as by remote monitoring and valid parameters are presented in one field or another. For example, the parameters Timeout and Retries (Retries) are useless in local monitoring (local checks) but are important in remote monitoring.

- Custom ID: Field to store a custom identification value.
- Unit: Choice of the unit of the data received by the module, empty by default. You can either choose a specific unit (Timeticks, Bytes, Entries, etc.) or click the pencil icon to set custom units.
- Interval: Period in which the module should return data. If a module goes more than two intervals without receiving data, it will enter an unknown state:

1. If they are remote modules: period in which the remote check is carried out.
2. If they are data modules: numerical value that represents X times the interval of the defined agent, performing the local check in that period.
3. In the case of Broker Agents via Web Console, from version 776 onwards, their interval is not displayed to prevent unwanted changes.

- Post process: Allows you to establish a conversion of the data received by the module (post-processing of the value). By default disabled (0). There are predefined options when installing Pandora FMS and you can also set custom conversions by clicking on the pencil icon.
- Min. Value and Max. Value: Allows you to set an expected minimum value and maximum value for the module.
- Dynamic Threshold Interval: Fields reserved for Dynamic monitoring (Dynamic Thresholds).
- Export target: If you have configured a export server, you can set one.
- Discard unknown events: Allows you to discard unknown events.
- FF threshold: Allows setting thresholds for the FlipFlop protection. FlipFlop (FF) is known as a common phenomenon in monitoring, when a value oscillates frequently between alternative values (BAD/GOOD). When this happens, a “threshold” is usually used, so that to consider that something has changed its state, it has to “remain” more than X consecutive intervals in a state without changing. FF Threshold is used to “filter” the continuous changes of state in the generation of events/states: this way Pandora FMS “knows” that until an element is not at least X times in the same state, after changing from an original state , do not consider it as having changed.
    - FF Interval: Allows to specify a shorter time interval for the next check if a Flip Flop threshold is activated in the module. When FF is enabled and a change of state is detected that meets the

set check conditions, the module interval for the next run will be adjusted. This setting facilitates faster checks when specific conditions are needed by setting a value smaller than the main module interval.
    - FlipFlop timeout: Timeout only used in asynchronous modules. For a state change by FF to be effective, equal consecutive data must be received within the specified interval.

For the calculation of the Service Level Agreements (SLA), if SLA thresholds are not set, Pandora FMS will take into account the FF threshold.

- Tags available and Tags from policy: These are features of the Enterprise version. They are detailed in the next section "Tags".
- Quiet: The module will continue to receive information, but no type of event or alert will be generated ("silent" mode).
- Cascade Protection Services: Cascade protection service, parameter by which the generation of events and alerts would pass to the service to which it belongs, if this cascade event functionality is enabled.
- Critical instructions, Warning instructions and Unknown instructions: Contains the instructions to follow if the module status changes to critical, warning or unknown. Useful in using Templates and Components.
- Cron: You can specify periods of time in which the module will be executed. It has the nomenclature: Minute, Hour, Day of the Month, Month, Day of the week. There are three different possibilities:
    - Cron from: Has stableDefault in all its fields Any (_Cualquiera_), without any time restriction for monitoring.
    - If Cron from → some specific value and Cron to all on Any: will be executed only when it matches the stipulated number. Ex: `15 20 * * *`, it will only be executed every day at 20:15.
    - Cron from → some specific value and Cron to → → some specific value: will run during the stated interval. Ex: `5 * * * *` and `10 * * * *`, will be executed every hour between 5 and 10 minutes (this is equivalent to `5-10 * * * *`).
    - Timeout: Time that the agent waits for the execution of the module, expressed in seconds.
    - Retries: Sets the number of retries for the execution of the module.
- Category: This categorization has no effect from the normal user interface. It is intended to be used in conjunction with the Metaconsole.
- Module parent: It is used to establish hierarchy in the protection in the cascade protection service (Cascade Protection Services).
- Custom macros : Any number of module macros can be defined. The recommended format for macro names is as follows: `_macroname_` .

These macros can be used in module alerts and are especially useful in WUX Monitoring and User Monitoring. If the module is of type web module analysis:

Dynamic macros will have a special format starting with @ and will have these possible substitutions:

- `@DATE_FORMAT` (current date/time with user defined format)
- `@DATE_FORMAT_nh` (hours)
- `@DATE_FORMAT_nm` (minutes)
- `@DATE_FORMAT_nd` (days)
- `@DATE_FORMAT_ns` (seconds)

- @DATE_FORMAT_nM (month)
- @DATE_FORMAT_nY (years)

Where “n” can be an unsigned (positive) or negative number and FORMAT follows the standard of perl strftime.

- Module relations: Used to replace the module, either directly (Direct) or on failover (Failover), for the purposes of SLA calculation.

Module tags

Management menu → Profiles → Module tags.

Tags are tags associated with each module that will then be propagated to the events that this module generates and can be used in event alerts from this module. They allow to be used as filters in reports, event views and even have specific views for them and can be used in alerts, since they are available as macro.

They can also be used to grant specific access permissions to a module, so that a user can access only one module of the agent, without having access to the rest of modules.

Dynamic Monitoring (Dynamic Thresholds)

Dynamic monitoring consists of the dynamic and automatic adjustment of module state thresholds in a predictive manner. The operation mode consists in collecting the values for a given period and calculating the average and a standard deviation, which are used to set the corresponding thresholds at the module level. Parameters are located in the advanced options of the modules:

- Dynamic Threshold Interval: Dynamic threshold interval or amount of time that will be considered to perform threshold calculation. If a month is chosen, the system will take all the existing daa for the last month and will build the thresholds based on that data and thresholds will be established with values above the average.
- Dynamic Threshold Max.: Maximum value of the critical dynamic threshold, if a tolerance margin is set (in percentage) for it; For instance, if the average values are around 60 and the critical threshold has been set from value 80, if the value Dynamic Threshold Max: 10 is set, this critical threshold will increase by 10%, so it would remain at a value of 88.
- Dynamic Threshold Min.:It allows you to reduce the lower limit by the percentage indicated. For example, if the average values are around 60 and the lower critical threshold has been set to a value of 40, if the value Dynamic Threshold Min: 10 is set, this critical threshold will be reduced by 10%, so it would take a value of 36.
- Dynamic Threshold Two Tailed: These are dynamic threshold intervals, which are disabled by default. If this option is activated, the dynamic threshold system will also set thresholds below the average.

Module Library

Available from version 744. Accessing the module library from the menu will require Agent Read (AR) permissions.

Access Management → Module library → View to access the main view. You can also group by categories (databases, virtualization, etc.) or search for the plugin by its name in the Search text box.

The download links of the Enterprise modules of Pandora FMS will only be visible in these cases:

- The username and password that has been configured in the setup must match the one of Integria IMS support.
- The version of Pandora FMS is Enterprise.
- The Pandora FMS user has AW permission.

Back to Pandora FMS documentation index