Introduction

Introduction

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

What is Pandora FMS?

Pandora FMS is a monitoring software oriented to all kinds of environments. It is oriented to serve in all types of roles and organizations. Your goal is to be flexible enough to manage and control your entire infrastructure without investing time or money in other tools.

FMS is an acronym for “Flexible MMonitoring System”.

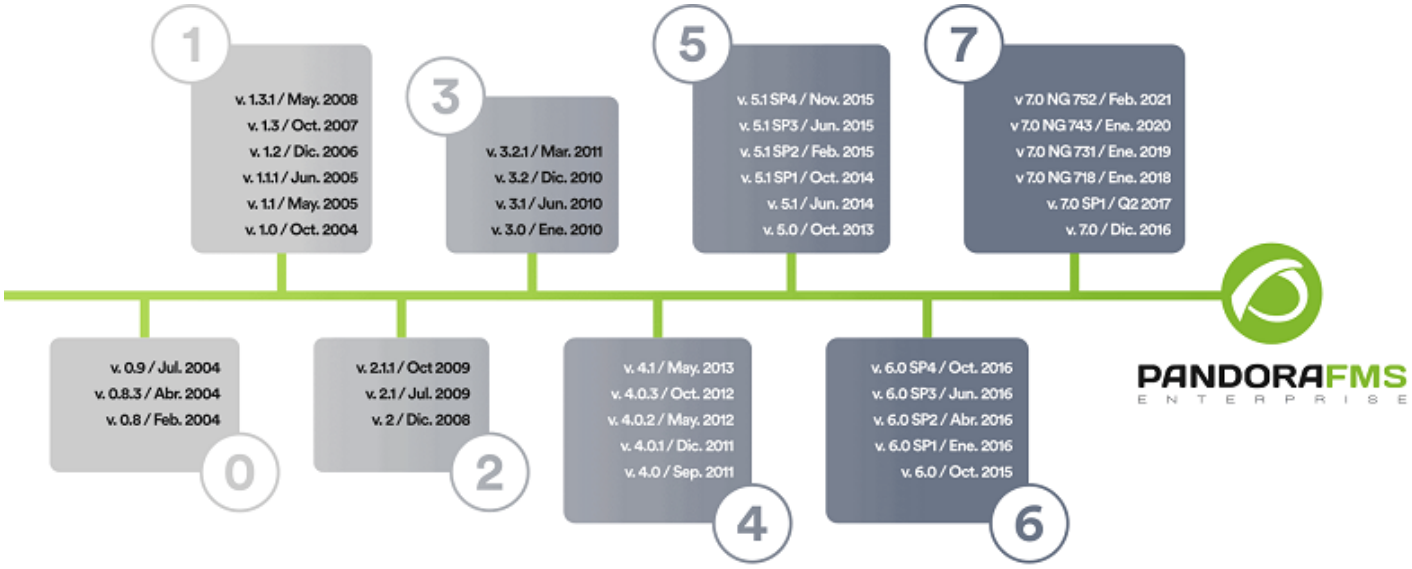
Pandora FMS currently has agents for all operating systems on the market. It can be used successfully not only to monitor systems, but also all kinds of network devices, either using SNMP, through TCP, ICMP and UDP protocol probes or Software Agents .

About the documentation

- In addition to this official documentation there is a user forum where you can ask questions.
- There is an official training program with certification, taught by the people who develop Pandora FMS.
- The quick guides help to configure Pandora FMS and implement simple monitoring, as well as to install software agents, both for GNU/Linux® and for MS Windows®.
- You can consult more information on our website: https://pandorafms.com/es.

The evolution of the Pandora FMS project

Pandora FMS was born from a personal development of its original author, Sancho Lerena, in 2003. Initially it was 100% open source and over the years the need arose to offer a version oriented to large companies: Pandora FMS Enterprise, capable of processing large volumes of information through the Metaconsole.



A look at the features of Pandora FMS

- Self-monitoring: By default it allows detecting storage devices or databases (BB.DD.) in a BB.DD. server, among other things.
- Auto discovery: Remotely by network you can detect all its elements, catalog them according to operating system (O.S.) and monitor with an assigned profile.
- Agents: They can obtain information from the execution of a command to the lowest level call of the MS Windows® API: events, logs, memory consumption, CPU usage, etc. PFMS has a library of default checks for speed.
- Control: The agents themselves can start services, delete temporary files or run processes. In the Enterprise version it can be done from the Web Console, remotely executing tasks such as stopping or starting services, including periodic executions. Furthermore, Pandora FMS can be used to remotely access remote systems thanks to eHorus (Telnet, VNC or SSH).
- Alert and notify: As important as detecting a failure is notifying it. With Pandora FMS there are several ways and notification formats available.
- View and analyze: Although monitoring is receiving an SNMP trap or viewing an interrupted service, it is also presenting trend reports, summary graphs of data collected over months, generating user portals, delegating reports to third parties or define your own graphs and tables.
- Inventory: Contrary to other solutions, where the CMDB concept is the base, for Pandora FMS this is optional. Inventory is flexible and dynamic, can be self-discovered, checked remotely, and so on. You can also notify changes, such as uninstalled software on a computer, or use it to create listings.

Remote Monitoring

When talking about remote monitoring, it refers to the fact that the Pandora FMS server is the one that polls, regularly or synchronously, the devices that you want to monitor. This synchronous polling process is known as polling or remote monitoring.

Remote monitoring is generally used:

- To verify that they are active and running.

- To obtain a numerical value (for example to measure network traffic or number of active connections).

This monitoring, when it is synchronous, is always carried out in the same direction: from the monitoring server to the monitored element and can be carried out with the most widespread protocols, SNMP and WMI (MS Microsoft®).

When it is the opposite case it is monitoring asynchronous, and is generally referred to as SNMP traps.

- To monitor network environments the protocol to choose is SNMP with an 'external' explorer of SNMP devices, access to the MIB collections of the manufacturers of their network devices (OID libraries) and listening for traps. Then the “custom” OID collections of each device will be added. For Unix® and GNU/Linux® systems, it must be taken into account to activate the SNMP functions.
- For MS Windows® servers, WMI remote monitoring is very appropriate and powerful since it is done with authentication credentials.

Finally, you can always monitor network elements by using TCP (for example: HTTP protocol or SMTP protocol) or ICMP (for example: ping or latency time) tests.

Local monitoring (with software agents)

When talking about systems and applications, the best way to obtain information is directly about the system, executing commands or consulting the system's data sources from the machine itself to be monitored. To execute some kind of command, script or make some kind of query about the system or application, the Software Agent of Pandora FMS is used.

Software Agents, in addition to their essential function of obtaining information through commands, include another series of advanced functions, such as obtaining inventory information. They can also be configured to act proactively in the event of a problem or failure, automatically interacting with the system, deleting a temporary file or executing a command. When a Software Agent cannot have direct contact with the designated Pandora FMS server, it may use a Satellite Server PFMS or an agent broker.

Monitoring procedures

Before beginning a deployment stage, it is important to consider which are the critical and most important points of the technological platform that is going to be monitored. In this way, before having specific data information about the systems, it is possible to know what to do with them and how to exploit the entire utility without wasting time on investigations or more trivial details.

- Availability: Event-based monitoring is of interest above all, and remote monitoring is probably sufficient; it is faster to deploy and results can be obtained in a short time. The SLA reports will be the most useful in this case.
- Performance: Are the graphs and the numbers; you can get that information with both agents and remote checks, but agents are probably needed to get detailed information from the systems. Grouped reports and combo charts take precedence.
- Capacity Planning: Much more specialized; It is necessary to obtain data, as in the second case, with predictive type monitors and very specific projection reports. Establishing early alerts will be very helpful, and you will need to know the concepts of WARNING and CRITICAL states well, in addition to developing a series of event management policies that allow you to anticipate the problem before it happens, without a doubt the most complex and interesting case. .

Action procedures

In order to develop action procedures, the following must be taken into account:

- Criticality of the event: Being able to discriminate something habitual from something infrequent or critical.
- Method of notification: email, SMS, Telegram, sound alert, etc.
- Escalated: Different forms of warning after the repetition of a problem. A common case is the notification to a person in charge after a certain time without solving a problem.

Before entering configurations, it is advisable to be clear about these concepts, draw up diagrams with the critical elements, how to monitor them, what to do with all the information collected and how to report any problems that appear.

Supervision models

- The direct supervision model implies that there is one or several people constantly observing the system. They can probably see small, non-critical changes and have a lot more flexibility. It is not necessary to define alerts for each possible case, it is enough to observe the last events to see what is happening in the system at that moment. In large environments this model is used.
- The indirect supervision model implies the use of previously configured automatic notifications. This system is suitable for few devices or when the critical elements are very well identified with their notification and pre-established solution.

Back to Pandora FMS Documentation Index