Pandora FMS Architecture

Pandora FMS Architecture

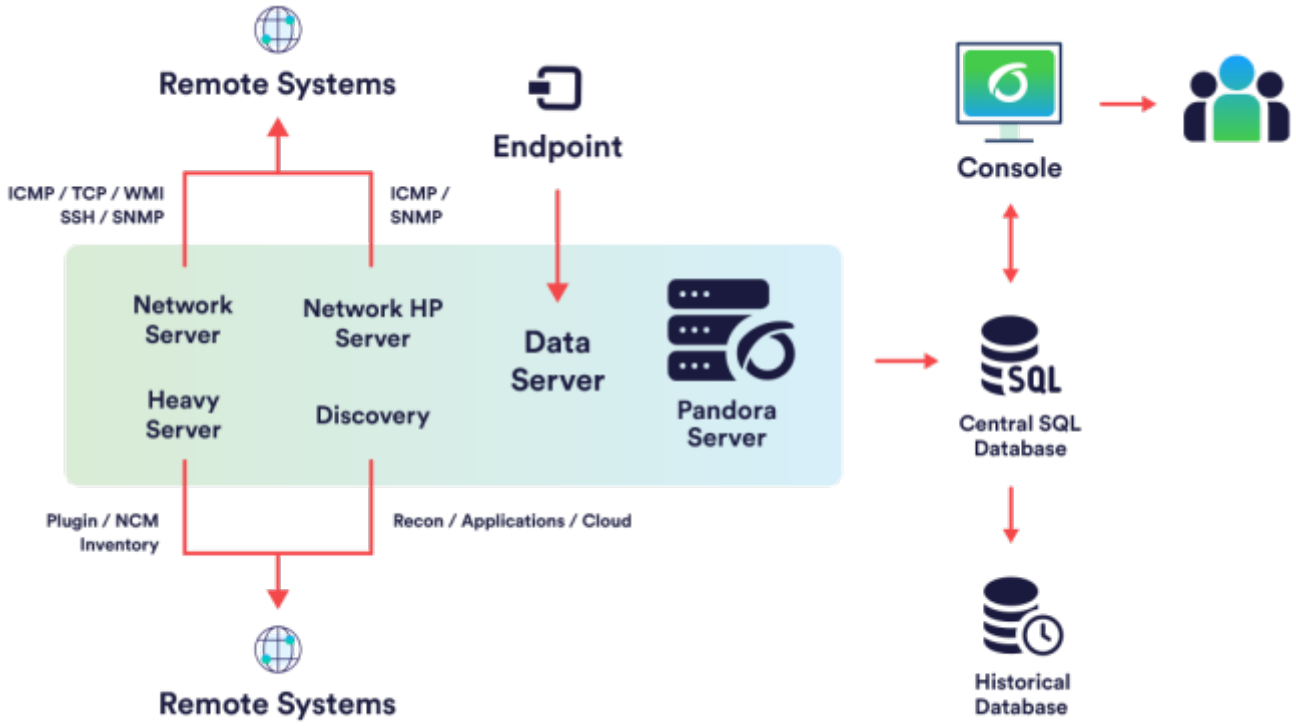
Introduction

The key component and where almost all the information is stored is MySQL database. All Pandora FMS components may be replicated and work in a fully HA environment (Active/Passive) or in a group or cluster environment (Active/Active with load balancing).

The PFMS Servers, with the information generated by themselves or by Agents, enter the data and information in the database. The Web Console is the part in charge of displaying the data and interacting with end users. EndPoints are applications that run on monitored systems and collect information to send it to Pandora FMS Servers.

Pandora FMS Servers

Servers are integrated into a single application, called Pandora Server as an ensemble, which is a multi thread application that runs different instances or specialized servers Pandora FMS at the same time. These are the elements in charge of carrying out the existing checks, since they verify and change their status based on the results obtained. They are also in charge of triggering the alerts that are established to control data state.



Concurrent servers may exist; one of them is the main server and the rest of the servers are secondary servers. Although there is a secondary and a main server, they all work simultaneously. The difference between the two is that when a server of the same type goes offline (for example, a Network Server) the main server is in charge of processing all the data associated with the offline server.

Pandora FMS automatically manages each server status, its load level and other parameters. Users may monitor the status of each server through the server status section of the Web Console.

See also:

- Server architecture (version 784).
- Sync Server.
- SIEM Server.
- Network monitoring with NetFlow and sFlow.
- Policy Manager.
- MADE Server.

Data Server

It only processes the information sent by EndPoints through Tentacle and API 2.0, which build an information package in XML format and deliver it to a specific directory that the Data Server processes first and then stores its result in the database.

Different data servers may be installed on different systems or on the same host using multi-CPU

virtual servers.

Despite its simplicity, the Data Server is one of the critical elements of the system, since it processes all the information from the agents and generates alerts and system events based on that data.

Network Server

Run remote monitoring tasks over the network: ICMP checks (ping and latency times), TCP requests and SNMP requests. It is very important for the machines running Network Servers to have «network visibility» (connection) to the devices to be remotely monitored.

This server also handles other tasks:

- WMI is a Microsoft® standard for obtaining operating system information and applications from MS Windows® environments. This is the dedicated server for monitoring remotely MS Windows® systems using the WMI protocol.
- An Artificial Intelligence component that implements a statistical data forecast based on past data up to 30 days old, allowing to predict data values with an interval of 10 to 15 minutes, and to find out whether a data at the current moment is anomalous compared to its history. You basically build a dynamic baseline with a weekly profile.
- Perform complete web checks, such as the user identification process, passing parameters by form, content checking, menu navigation, etc. It is used for true/false availability checks and to obtain full browsing experience latency times.

SNMP trap Server

This server uses the standard trap collection system daemon, snmptrapd: It receives SNMP traps and Pandora FMS SNMP Console processes and stores them in the database. It is also in charge of launching the alerts associated with SNMP traps that were defined.

Discovery Server

Formerly called the Recon Server, the Discovery Server is used to regularly scan the network and detect new running systems and apply a monitoring template and start monitoring immediately. By means of the GNU system applications nmap, xprobe and traceroute, it is able to detect Operating Systems and establish a network topology.

The Discovery Server is also used to launch scheduled tasks and launch specific monitoring

against virtual environments, databases or all those applications or environments that require exploring what exists before monitoring.

Event Server

This special server is used to correlate events and generate alerts and does not execute monitoring tasks. This server, unlike the rest, does not have thread configuration or high availability.

Satellite Server

It is installed separately from the main Pandora FMS Server and allows forwarding data files from EndPoints to the main server, working as agent proxy in distributed topologies. It sends monitoring data as XML files through a Tentacle connection, so it does not require connection to the database.

WUX Server

Combined with the Selenium Grid allows complex web transactions to be carried out in a distributed manner. These transactions are executed in a real browser, their output is captured and processed for step-by-step viewing, including error traps and detailed statistics.

Syslog Server

It allows analyzing the syslog of the machine where it is located, analyzing its content and storing the references in the corresponding OpenSearch Server.

Log Server

It allows you to correlate logs and run your alerts.

Alert Server

If it is activated, it will be in charge of executing all monitoring alerts, since by default each server is in charge of its own alerts and in some specific cases, there may be delays in monitoring if an

alert must execute a task and it takes longer of what is due to be done.

Heavy Server

Heavy Server runs complex checks remotely through custom scripts, managed centrally. This allows an advanced user to define their own complex tests and integrate them into the application so that they may be used conveniently and centrally from Pandora FMS.

It also performs additional functions:

- It supports everything necessary for Network Config Management (NCM).
- It obtains and displays inventory system information: Installed software, model of hardware elements, storage devices, running services, etc. It may retrieve this information both remotely and locally.
- It allows exporting the data of a monitored device from a Pandora FMS installation to another, and thus have the data replicated. Especially useful in large deployments with several Pandora FMS installations and the need to centralize.

Network High Performance Server

Network HP Server uses advanced strategies to perform ICMP (ping) and SNMP bulk checks, resulting in high performance.

Pandora FMS web console

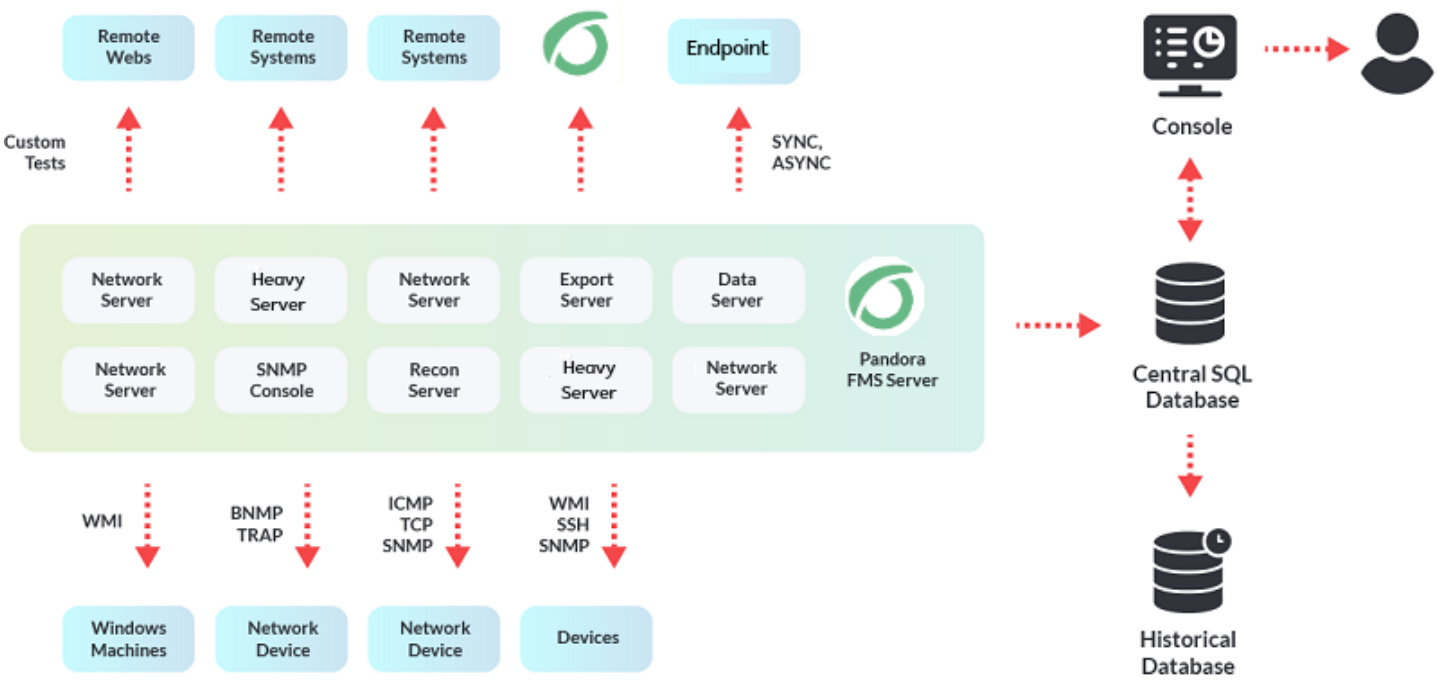
It is Pandora FMS user interface. This Management and Operation Console allows different users, with different privileges, to control Agent status, see statistical information, generate graphs and data tables, as well as manage incidents with its integrated system. It is also capable of generating reports and centrally defining new Modules, Agents, alerts and creating other users and profiles.

It may run on multiple servers to spread load as well as to ease access due to logistical issues (large networks, many different user groups, geographic differences, administrative differences, etc.).

Pandora FMS Database

Pandora FMS uses a MySQL database in which it stores all information received in real time,

normalizing all the data from the multiple sources. Currently Pandora FMS only supports MySQL, MariaDB and Percona.



Pandora FMS EndPoints

It is important to differentiate between two concepts: Agent, or Console Agent, as a container, and EndPoint, which is installed and runs on a computer.

Agent (Container)

Pandora FMS Agent is an organizational element created in Pandora FMS Web Console, associated to a group of Modules (or individual monitoring elements). This agent may (optionally) have one or more IP addresses associated with it.

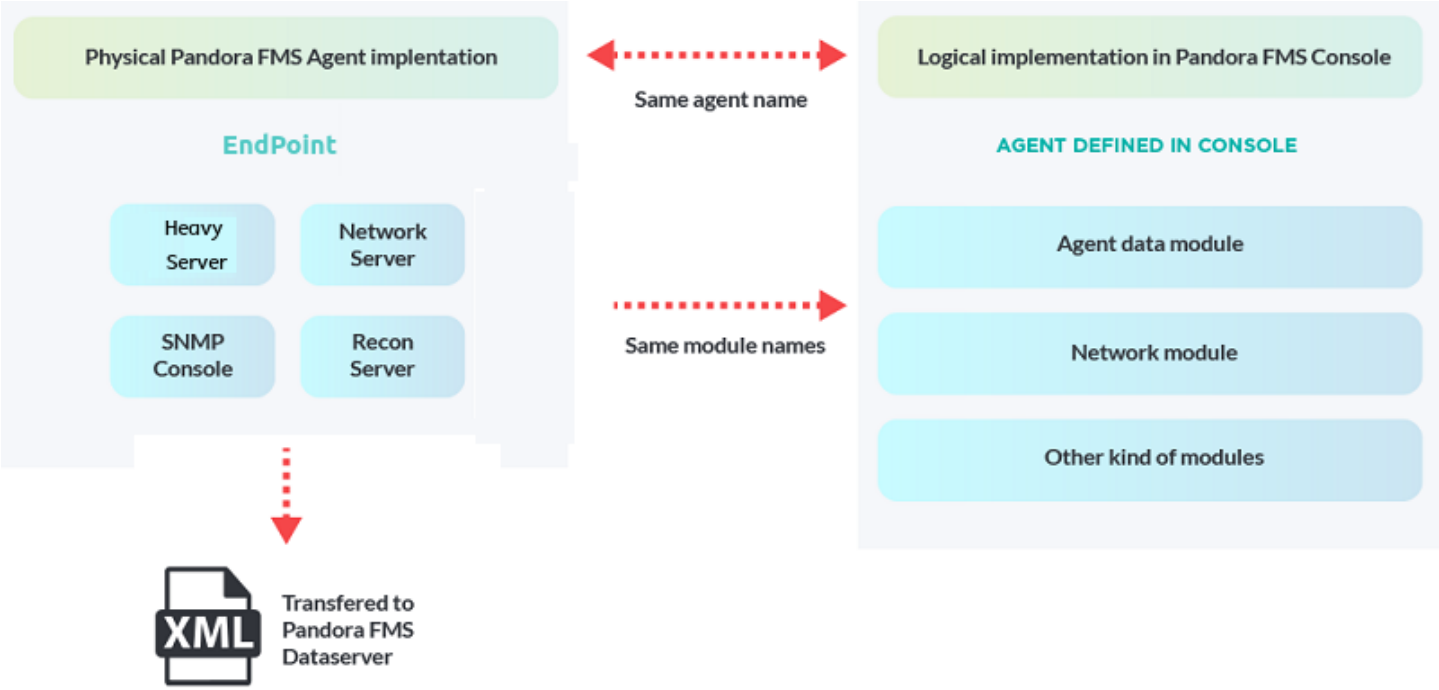
An Agent may contain remote or local Modules. Remote modules are run by those servers that obtain information remotely (such as the Network Server); local modules are run by EndPoints and collected and processed by the Data Server.

EndPoint

EndPoints are installed locally on the computers to be monitored, retrieving information from the

computer itself. They are mainly used in servers to monitor machine resources (CPU, RAM, disks...) and installed applications (MySQL, Apache, JBoss...). Generally, server and equipment monitoring will be carried out with EndPoints while monitoring of network equipment will be done remotely without installing any software.

All the information of the checks carried out is reflected in a single data file in XML format, which is sent through the Tentacle protocol to Pandora FMS Server at a predetermined interval of 300 seconds. It is also possible to transmit the packages using SSH or FTP.



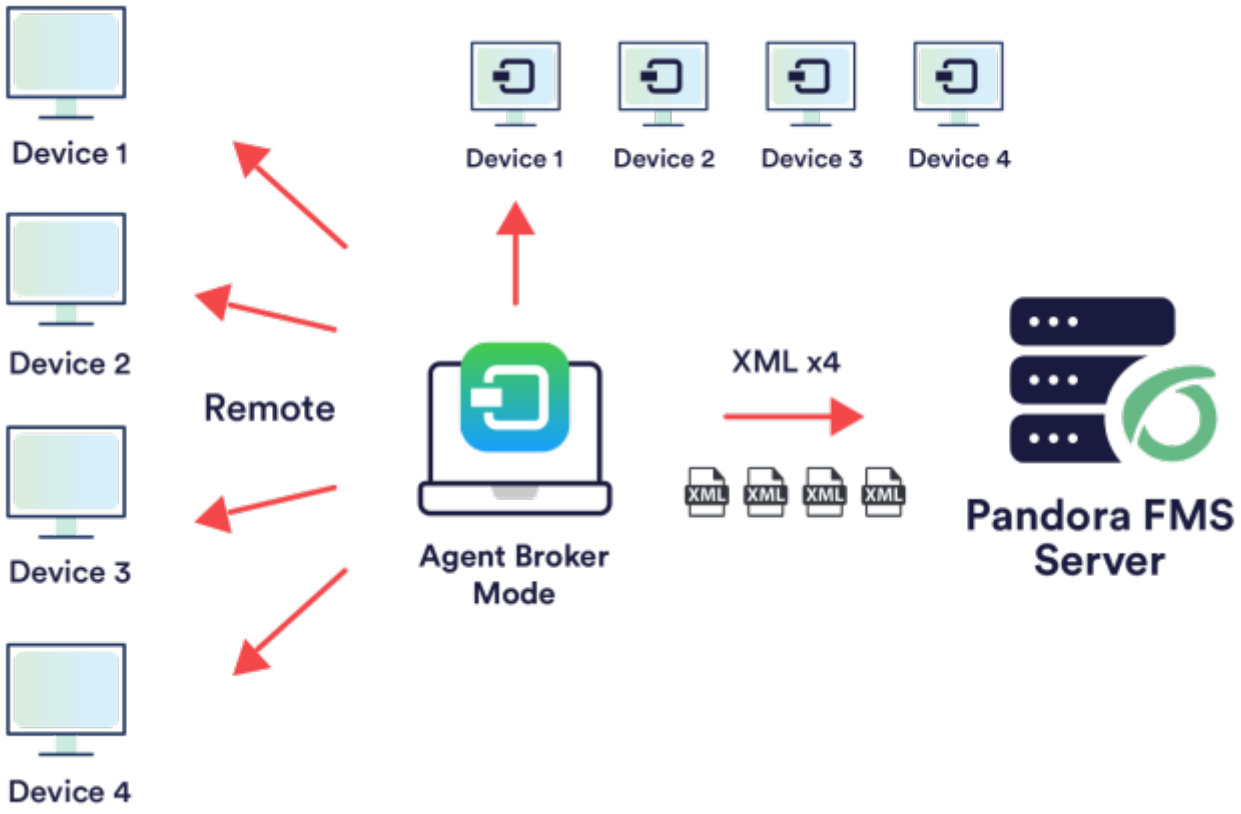
Topologies, schemes and monitoring models

Accessible networks

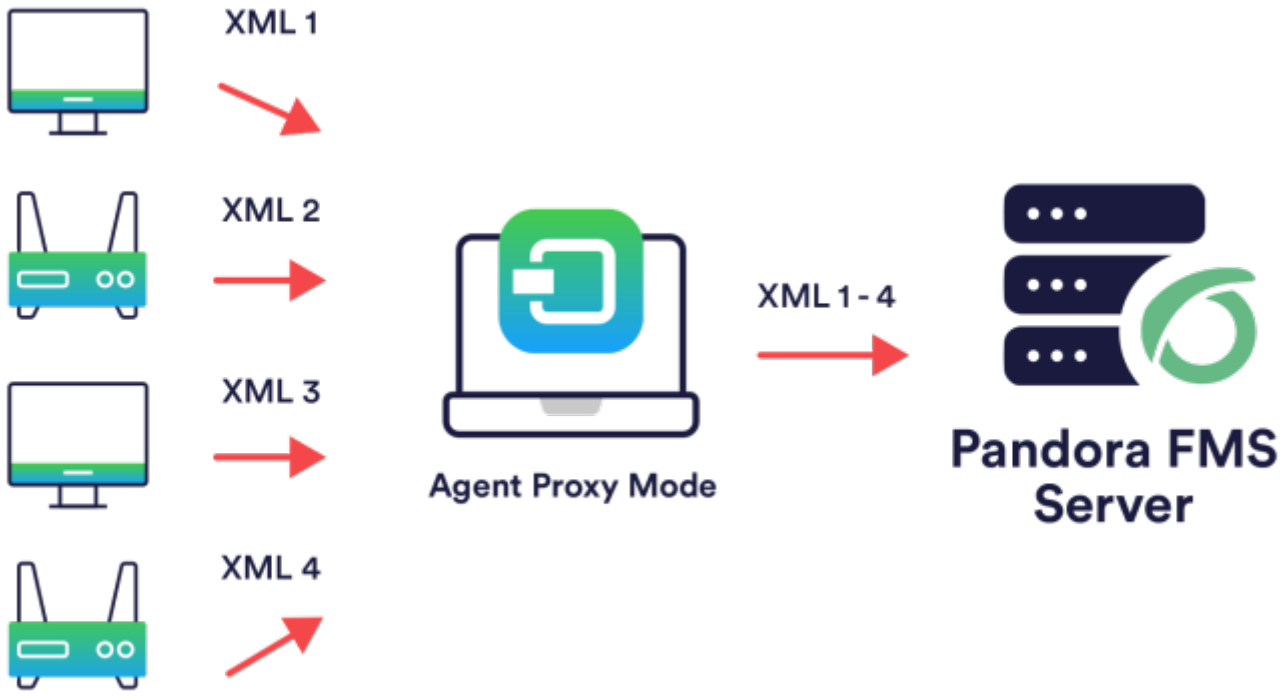
- Accessible network for centralized remote monitoring: where, from Pandora FMS Server, you may access all the machines and/or devices to probe remotely.
- Accessible network for Agent-based monitoring: where, from the EndPoints installed on monitored machines, they may reach Pandora FMS Server without problems.

Networks with difficult access

- Remote network not reachable by Pandora FMS remote checks: It uses the broker agent mode.



- EndPoints that do not have access to Pandora FMS Server: This case uses the EndPoints proxy feature or a Satellite Server as EndPoints proxy.



- Need to monitor different networks for remote monitoring with the server: In this case you may also use the Satellite Server or several different Pandora FMS Servers connected to the same database.

Special organizational features

- Reporting duality: Additionally, you may configure Agents to report to two different Pandora FMS Servers, although it may only be managed by one of them.
- Fragmented management: It is necessary to delegate the management of part of the teams to different personnel, with different accesses. This, more than an architecture problem, is a management problem. It is solved with assigned permissions on policies.

Large environments with Pandora FMS

- Large network: When they cannot be centralized into a single server, servers in broker mode are used, which distribute the load of remote checks.
- Redundant servers: For safety, should the primary hardware fail, a server in HA mode may automatically relocate and delegate the monitoring workload.

←Back to Pandora FMS documentation index