PANDORAFMS

Configuration

21-09-2021

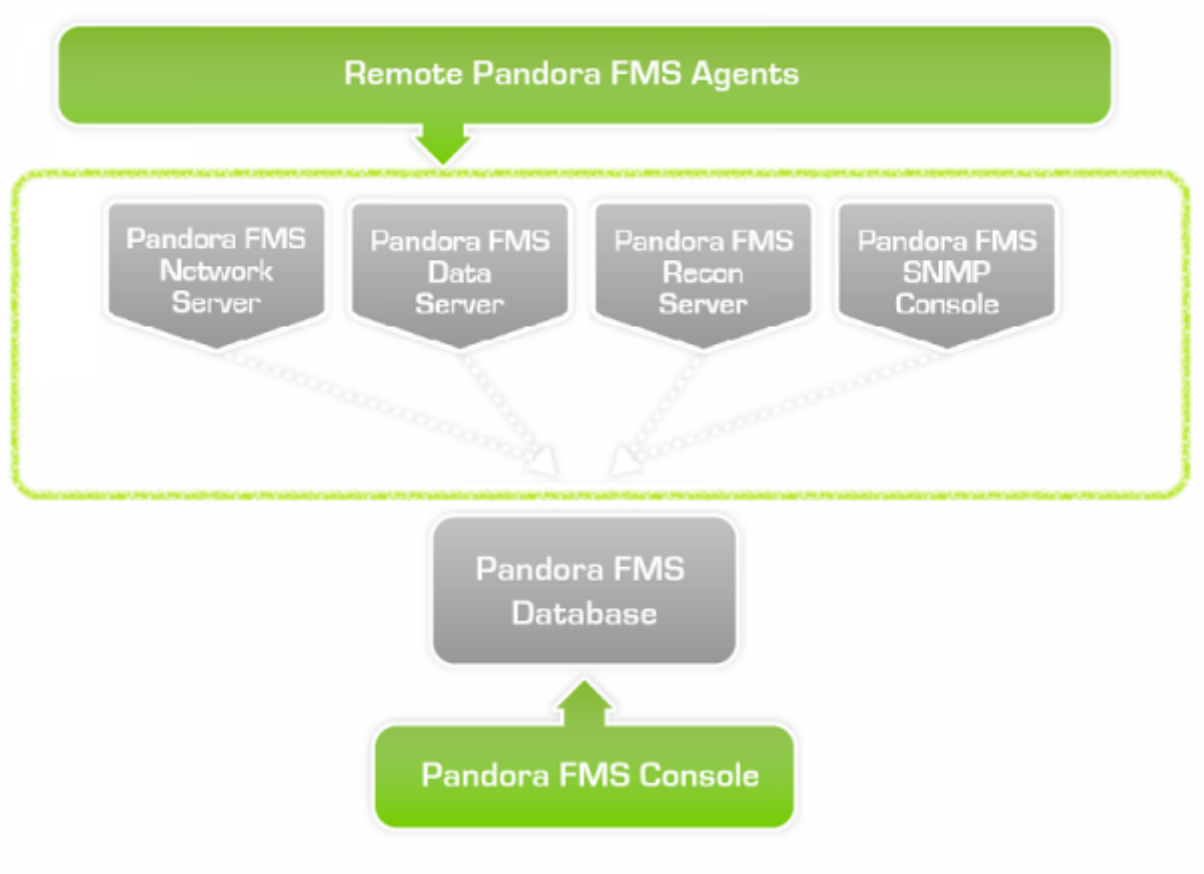
Configuration

Go back to Pandora FMS documentation index

Pandora FMS has three essential components essential to configure correctly for good functioning, which are the web console, the server and the database.

Even if you already have a Pandora FMS installed and running, if you have installed it through the **appliance software** , consider adjusting and revising the configuration for a much more optimal operation.

You may get more information about Pandora FMS optimizationin this section. In this chapter, we are going to explain the configuration files of the three elements and others which are important for a correct performance of the application components.

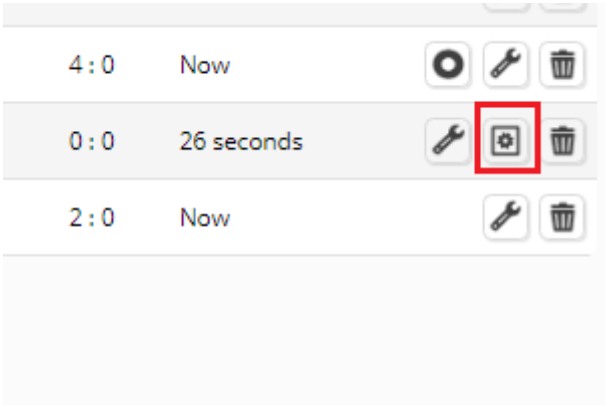


Server

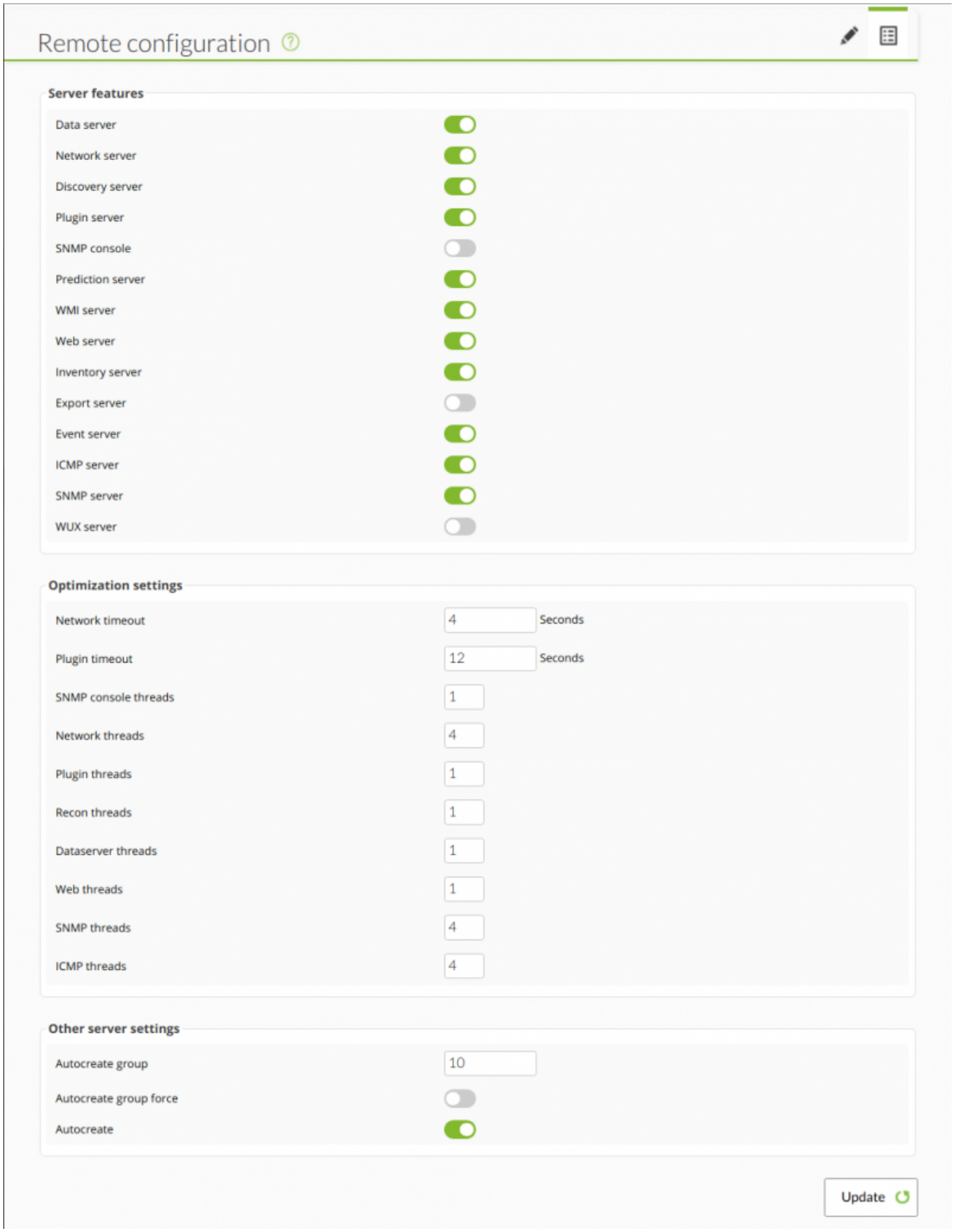
Pandora FMS server main configuration can be found in the file `pandora_server.conf` is located at `/etc/pandora` by default.

From Pandora FMS version 7.0NG.752 onwards, it is possible to make some modifications related to the Pandora FMS server using a graphical interface, without the need to access the configuration file in plain text (neither through terminal nor from the web console).

To do this, the remote configuration should be previously enabled inside the `pandora_server.conf` configuration file. You should access to the servers view, and then click on the remote configuration icon enabled in the data server line.



There you may find in the first section, **Server Features**,a token next to the server to enable or disable it accordingly.



There is also a second configuration part, **Optimization settings**, devoted to optimization settings. In this section you will be able to modify parameters such as the timeout times or the threads dedicated to the servers.

And finally, a space reserved for other configurations: **Other server settings**. This

section includes the possibility of indicating the group ID to which the agents that are added to the Pandora FMS environment will be assigned by default if one is not specifically indicated during its creation. Force auto-creation and enable agent auto-creation when receiving data files with an agent ID that does not exist in the system.

Configuration File Elements

It is a UNIX standard plain text file, where unused variables or comments are preceded by character #. If you are editing from MS Windows®, make sure to use an editor that supports that format. Eventually, if you need to encrypt specific characters check the Pandora FMS Change remote config encoding parameter. All file configuration parameters are listed below.

See the Security Architecture section **to ensure the operation** of the entire Pandora FMS system.

servername

It is the name that the server will have when it is displayed in the console. By default it is commented and uses the name of the machine for the operating system.

Changing the name once it is running could cause remote checks to stop working, since the default server would have to be reconfigured in all existing agents to use the new server, as well as deleting the old server name from the server list.

incomingdir

It is the incoming directory of XML data packages. It is located under `/var/spool/pandora/data_in/` by default. This allows setting up a RAM disk or a very fast hard drive here (SSD, for example) to optimize Pandora MFS.

log_file

The Pandora FMS record file (log). It is located under `/var/log/pandora/pandora_server.log` by default. This is the main log file and it is very important for debugging.

snmp_logfile

Located under `/var/log/pandora/pandora_snmptrap.log` by default. This is a log file from SNMP console that contains all received SNMP traps BEFORE Pandora FMS server processes them.

errorlog_file

The Pandora FMS error registry file (log). It is located under `/var/log/pandora/pandora_server.error` by default. This log file stores all non-controlled errors or non-captured output from tools executed by the server.

daemon

It shows whether or not Pandora FMS server is executed as a daemon. If the server is launched with the –D option, it is executed as daemon.

dbengine

Deprecated: always `Mysql` (default value, MySQL is Pandora FMS database software).

dbname

Database name to which the server will connect. The default value is `pandora`.

dbuser

Username used in the Pandora FMS database connection. It is `pandora` by default.

dbpass

Password for the connection to Pandora FMS database.

dbhost

IP address or equipment name which hosts the Pandora FMS database. In a reduced installation, it is usually on the same equipment as that of the server, which is `127.0.0.1`.

dbport

TCP port where the the database engine listens (optional). `3306` is set by default if the value is commented.

verbosity

It is the level of detail for server logs. Possible values range from 0 (off) to 10 (maximum level of detail). With a value of 10, the log will show all the executions that the server performs, including modules, plugins and alerts.

The use of high values is not recommended on an ongoing basis due to the large growth of log files, which can cause performance problems in the system.

master

Master server priority. The server with the highest value (a numerical value, positive and without decimals) that is running will be the master. Ties are resolved at random. If set to 0, this server will never become a master. See the High Availability (HA) chapter for more information.

snmpconsole

Enabling it (value 1) indicates that the SNMP trap reception console is enabled in the

configuration. `0` that it is not. The console depends on the UNIX `snmptrapd` service and stops and starts it when Pandora FMS boots. Before starting Pandora FMS, verify that the `snmptrapd` process has not been started in the system.

snmpconsole_lock

If set to `1`, traps from the same source will never be processed in parallel. `0` by default.

snmpconsole_threshold

Time between consecutive reads of the SNMP log file in seconds. Defaults to `server_threshold`.

snmpconsole_threads

Number of threads for the SNMP Console. Each thread processes an SNMP trap. Set to 1 by default.

translate_variable_bindings

E If set to `1`, the SNMP console will attempt to translate variable `bindings` when processing SNMP traps. Set to `0` by default.

translate_enterprise_strings

E If set to 1 (default value), the SNMP console will attempt to translate enterprise strings when processing SNMP traps.

snmp_ignore_authfailure

Snmptrapd will ignore the `authenticationFailure` traps in case of it being activated, `1` (default value).

snmp_pdu_address

If enabled (value 1) Snmptrapd will read from the **Protocol data units** (PDU) address

instead of the agent address. Its value is `0` by default.

snmp_trapd

Path to the `snmp_trapd` binary. If set to manual, the server will not attemp to start `snmp_trapd`. Its value is manual by default.

snmp_forward_trap

Enables (`1`) or disables (`0`) SNMP trap forwarding to the host specified in snmp_forward_ip.

snmp_forward_ip

IP address of the host to which SNMP traps will be forwarded to.

Bear in mind that setting a forwarding address to Pandora FMS itself will cause a forwarding loop that will make the Monitoring Server collapse.

snmp_forward_version

SNMP version to use when forwarding SNMP traps. This token can only have the following values:

- 1
- 2c
- 3

snmp_forward_secName

Only for SNMP version 3. It defines the authentication security name. More information at snmpcmd's guide (man style help).

snmp_forward_engineid

Only for SNMP version 3. It defines the authorized **engine ID**. More information at snmpcmd's guide (man style help).

snmp_forward_authProtocol

Only for SNMP version 3. It defines the authentication protocol. This token can only have the following values:

- MD5
- SHA

More information at snmpcmd's guide (man style help).

snmp_forward_authPassword

Only for SNMP version 3. It defines the authentication password. More information at snmpcmd's guide (man style help).

snmp_forward_privProtocol

Only for SNMP version 3. It defines the privacy protocol. This token can only have the following values:

- DES
- AES

More information at snmpcmd's guide (man style help).

snmp_forward_privPassword

Only for SNMP version 3. It defines the privacy pass phrase. More information at snmpcmd's guide (man style help).

snmp_forward_secLevel

Only for SNMP version 3. It defines the security level. This token can only have the following values:

- `noAuthNoPriv`.
- `authNoPriv`.

- `authPriv`.

snmp_forward_community

SNMP community to be defined (`public`, `private`, etc.).

networkserver

1 enables the Pandora FMS Network Server, `0` disables it.

dataserver

1 enables the Pandora FMS Data Server, `0` disables it.

The Data server is a special server that also performs other delicate tasks. If you have several Pandora FMS servers in your installation, at least one of them must have a `dataserver` thread running.

reconserver

Network discovery server, now called Pandora FMS Discovery server: enabled 1 or disabled `0`.

pluginserver

Pandora FMS remote plugin server: 1 enabled, `0` disabled.

plugin_exec

Shows the absolute path to the program which executes the plugins in a controlled way in time. The default value is `/usr/bin/timeout`. If your base system does not have this command, use `/usr/bin/pandora_exec` instead, which is included in Pandora FMS.

predictionserver

1 enables Pandora FMS Prediction Server, `0` disables it.

wmiserver

1 enables Pandora FMS WMI Server, `0` disables it.

network_timeout

It is the timeout -in seconds- for ICMP checks. Its value is 2 seconds by default. If you are going to perform checks on WAN networks, it is advisable to increase this value to avoid false positives taking into account that some checks may require more time.

The more timeout you have, the more time you will need to run checks in the worst-case scenario.

server_keepalive

It is the time -in seconds- before declaring the server down. Each server checks the status of the servers around it, and in case the date of last update of one of them exceeds this value, it will mark it as down. This affects, to how High Availability (HA) works, in the case of having several servers.

It is essential that if you have multiple servers, all their internal clocks are synchronized through NTP.

thread_log

Version NG 7 or superior.

Set to 0 unless you are debugging your Pandora FMS Server. 1 causes server threads to periodically dump their status to disk at:

```
/tmp/<server name>.<server type>.<thread number>.log
```

For example:

```
 [root_pandorafms]# cat /tmp/pandorafms.*
 2017-12-05 09:44:19 pandorafms dataserver (thread 2):[[CONSUMER]]
Waiting for data.
 2017-12-05 09:44:39 pandorafms dataserver (thread 3):[[PRODUCER]]
Queuing tasks.
 2017-12-05 09:44:40 pandorafms eventserver (thread
21):[[CONSUMER]] Waiting for data.
 2017-12-05 09:44:40 pandorafms eventserver (thread
22):[[PRODUCER]] Queuing tasks.
 2017-12-05 09:44:14 pandorafms inventoryserver (thread
17):[[CONSUMER]] Waiting for data.
 2017-12-05 09:44:39 pandorafms inventoryserver (thread
18):[[PRODUCER]] Queuing tasks.
 2017-12-05 09:44:14 pandorafms networkserver (thread
4):[[CONSUMER]] Waiting for data.
 2017-12-05 09:44:14 pandorafms networkserver (thread
5):[[CONSUMER]] Waiting for data.
 2017-12-05 09:44:14 pandorafms networkserver (thread
6):[[CONSUMER]] Waiting for data.
 2017-12-05 09:44:14 pandorafms networkserver (thread
7):[[CONSUMER]] Waiting for data.
 2017-12-05 09:44:39 pandorafms networkserver (thread
8):[[PRODUCER]] Queuing tasks.
 2017-12-05 09:44:14 pandorafms pluginserver (thread
13):[[CONSUMER]] Waiting for data.
 2017-12-05 09:44:39 pandorafms pluginserver (thread
14):[[PRODUCER]] Queuing tasks.
 2017-12-05 09:44:14 pandorafms predictionserver (thread
15):[[CONSUMER]] Waiting for data.
 2017-12-05 09:44:39 pandorafms predictionserver (thread
16):[[PRODUCER]] Queuing tasks.
 2017-12-05 09:44:39 pandorafms reconserver (thread
10):[[PRODUCER]] Queuing tasks.
 2017-12-05 09:44:14 pandorafms reconserver (thread 9):[[CONSUMER]]
Waiting for data.
 2017-12-05 09:44:15 pandorafms webserver (thread 19):[[CONSUMER]]
Waiting for data.
 2017-12-05 09:44:40 pandorafms webserver (thread 20):[[PRODUCER]]
```

```
Queuing tasks.
 2017-12-05 09:44:14 pandorafms wmiserver (thread 11):[[CONSUMER]]
Waiting for data.
 2017-12-05 09:44:39 pandorafms wmiserver (thread 12):[[PRODUCER]]
Queuing tasks.
```

server_threshold

The number of seconds for the main loop. Its value is '5' by default.

This is a very important value for server configuration, it defines how many times Pandora FMS will search to see whether there are pending data in the database or in the hard disk (to search XML files). 5 to 15 is a valid value in most cases. If set to 1, the CPU usage will go up a lot. You can use the value 1 for special occasions, such as when Pandora FMS has been stopped for some time and there are many XML files and network tasks to process. When set to 1, it will process the pending tasks a little faster, but when it is finished, it should be set between 5 and 15 again.

With very low values and high load, there will be an “overheating” effect that progressively increases the CPU and memory consumption of the server.

This value together with the `_thread` and `max_queue_files` parameters are used to configure server performance.

network_threads

Number of threads for the network server. It shows how many checks can be done at the same time, but as it increases it requires many more server resources. Having more than twenty threads requires having a machine with many independent processors or cores.

icmp_checks

It defines the number of pings to each `'icmp_proc` module. At least one of these checks has to return 1 to the module to be classified as correct. Its default value is 1. If you set '5' here and the first ping is OK, the other 4 will be skipped.

In case of networks that have limited reliability, it is recommended to key in 2 or 3. A higher number will cause the rate of checks per second to decrease significantly in the event of any network segment failure.

Do not mistake it with the `icmp_packets` parameter which refers to the number of packets within the ping itself. The `icmp_checks` value defines the number of pings, each with its `icmp_packets`.

icmp_packets

Defines the number of ICMP packets sent in each ping request. 1 by default.

tcp_checks

Number of TCP retries in case the first one fails. Its default value is 1.

tcp_timeout

Specific timeout for TCP connections. The default value is `30` seconds.

A high number (>40) will cause the rate of checks per second to decrease significantly in the event of a network segment failure.

snmp_checks

Number of SNMP retries in case the first one fails. The default value is 1.

snmp_timeout

Specific expiration time for SNMP connections. Its default value is 3.

A high number will cause the rate of checks per second to decrease significantly in the event of a network segment failure.

snmp_proc_deadresponse

Returns DOWN if it is impossible to connect with a boolean SNMP module (**proc**) or if it gets NULL as a response. If set to 0, it is ignored.

plugin_threads

Number of threads for the remote plugin server. It shows how many checks could be done simultaneously.

plugin_timeout

Timeout for checks with plugins. After this time, the module status will be shown as 'unknown'. Its default value is 5, but you may want to raise it to a higher value in case you have plugins that may take longer than that.

wmi_timeout

Expiry time of WMI checks. After this time, the module status will be displayed as unknown. Its default value is 10.

wmi_threads

Number of threads for the WMI server. It shows how many checks can be done

simultaneously.

recon_threads

Number of threads for the network recon server. It shows how many checks can be done simultaneously.

dataserver_threads

Number of threads for the data server. Shows how many XML files can be processed simultaneously. As a specific rule for the *dataserver*, a number of threads higher than the machine's physical processors should not be used.

In the specific case of the *dataserver*, a value higher than 5 or 6 does not imply better performance.

mta_address

Mail Server IP address (Mail Transfer Agent).

If you are using a Pandora FMS ISO installation and you want to use the Postfix server distributed in it, make sure that your Pandora FMS server is able to resolve through its DNS server the mail server in charge of your e-mail domain.

```
nslookup -type=mx my.domain
```

Also, make sure in this case that your mail server accepts the emails redirected from Pandora FMS server.

If not set, Pandora FMS Console configuration will be used. It is possible to have a different MTA

configuration for the Pandora FMS Server and the Pandora FMS Console.

mta_port

Mail server port (25 by default)

mta_user

Mail server user (if necessary for authentication).

mta_pass

Mail server password (if necessary for authentication).

mta_auth

Mail server authentication system if necessary; the supported values are:

- `LOGIN`.
- `PLAIN`.
- `CRAM-MD5`.
- `DIGEST-MD`.

mta_from

Mail address from which messages will be sent. The default value is `pandora@localhost`.

mta_encryption

Version NG 7 or superior.

SMTP connection encryption type (`none`, `ssl`, `starttls`).

mail_in_separate

1 by default. If set to 1, it delivers separate mail for each recipient. If set to 0, the mail will be shared among all recipients.

xprobe2

If provided, it is used to determine the operating system of the remote systems, when a recon network task is launched. The default path is `/usr/bin/xprobe2`.

nmap

Required for the Discovery server. The default path is `/usr/bin/nmap`.

fping

Required for the ICMP server. It is located at `/usr/sbin/fping` by default.

nmap_timing_template

A value that specifies how aggressive **nmap** should be, from 1 to 5. 1 means slower but more reliable, 51 means faster but less reliable. 2 set by default.

recon_timing_template

It is just like the nmap_timing_template, but applied to Satellite Server and Recon Server network scans.

snmpget

Required for SNMP checks. The default path is `/usr/bin/snmpget`. It refers to the location of the SNMP standard client for the system. In the case of Windows, a binary is provided for this purpose.

braa

E

Location of the **braa** binary required for the Enterprise SNMP server (default path is `/usr/bin/braa`).

braa_retries

E Number of retries before **braa** hands a module over to the Network Server in case of an error.

fsnmp

Version NG 7 or superior.

E Path to the **pandorafsnmp** binary, used by the Enterprise SNMP Server for SNMPv3 requests (`/usr/bin/pandorafsnmp` by default).

autocreate_group

Numeric ID of the default group for new agents, created with the data server through the datafile reception. If there is no defined group here, the agents will be created in the group containing the XML.

autocreate_group_force

If set to `1`, new agents will be added to the group specified by autocreate_group (the group specified by the agent will be used as fallback).

If set to `0`, new agents will be added to the group specified by the agent (the group specified by **autocreate_group** will be used as fallback).

For example, with the following configuration a new agent would be placed in the group specified in its XML data file if possible, or the group with ID 10 if not:

```
autocreate_group 10
```

```
autocreate_group_force 0
```

autocreate

Setting it to 1 will autocreate agents when data files with an agent ID that does not exist in the system are received.

If you want to set up a security mechanism, you can set a group password.

max_log_size

Maximum size of Pandora FMS log file, in bytes. When this size is reached, the log file's name is changed to `pandora_server.log.old` and the server generates a new one with the original name, `pandora_server.log`. Default size is 65 536 bytes.

max_log_generation

It specifies max generation count (between 1 and 9) of Pandora FMS server log files. The default value is 1.

max_queue_files

Maximum number of XML data files read by the Pandora FMS Data Server from the directory specified by incomingdir. This prevents the Data Server from trying to process too many files, which would affect server performance. The default value is 5000.

Incremental modules may not work properly if this value is not high enough to hold all the XML data files.

use_xml_timestamp

It is enabled (1) by default and it uses the date and time (timestamp) defined **inside the**

XML (`.data`), that is, the timestamp generated by the agent.

If disabled (`0`), it will use the timestamp of the XML file, that is **the server's timestamp**. This could be useful to **globally** disable the use of dates generated by agents and just use the server's date and time as a reference for all data, because this timestamp is generated right when Pandora FMS server receives the XML.

These settings changed in Pandora FMS 747 version. In previous versions this token is disabled by default.

There is a similar feature at agent level, so that the agent data gets evaluated with the date the file was received.

auto_restart

Deactivated by default. If activated (value in seconds) it forces the server to restart internally every N seconds (1 day = 86400). This option is useful if degradation is noticed due to the uncontrolled failure of some thread or specific Pandora FMS server.

restart

It is disabled by default (`0`). The server will restart in the face of critical errors after a few seconds.

restart_delay

The default value is `60`. The number of seconds the server will wait before restarting after a critical error if restart is enabled.

activate_gis

Enable (`1`) or disable (`0`) server GIS features.

location_error

Margin of error in meters to consider two GIS locations as the same location.

recon_reverse_geolocation_file

Recon reverse geolocation file. This file must be in MaxMind GPL format (`GeoLiteCity.dat` format). If this option is commented on in the configuration file, it will disable geolocation by IP when creating agents using recon and software agents. Geolocation will not be carried out either if the GIS features (activate_gis) are disabled overall.

recon_location_scatter_radius

Radius (in meters) of the circle where the agents are randomly placed when found by a recon task. The center of the circle is found out by geolocating the IP.

self_monitoring

The server has a self monitoring flag which creates an agent with the same name as the server, which monitors most of the important parameters of a Pandora FMS Server. To activate it, the parameter `self-monitoring` must be set to `1`.

self_monitoring_interval

Time interval for self_monitoring in seconds.

update_parent

Defines whether the agent can update its parent by sending the parent name in XML, but if the parameter is not set or is 0, then the agent information will be ignored.

If this is not the case, when the server receives an XML with the `parent_name` attribute, it searches for an agent with this name, and if it finds it, it updates the parent of the XML agent.

google_maps_description

This enables the conversion of GPS coordinates into a textual description of the position (reverse geolocation). This will be done using the Google Maps API. To be able to use this feature you need internet access, and you can have performance penalties processing GIS information due to the connection speed against Google API from Pandora FMS server.

The Google Maps API is a paid service and requires credentials, you will need to obtain the KEY API and pay, otherwise the service will be suspended after a couple of days of use.

openstreetmaps_description

This enables the conversion of GPS coordinates into a textual description of the position (reverse geolocation). This will be done using the OpenStreetMaps API. This service is not as accurate as Google Maps, but it is free. It also has the advantage that it can - through code modifications - be modified to connect to a local server.

If used with direct Internet connection (default), Internet access is required, and you can have performance penalties processing GIS information to the OpenStreetMaps API from Pandora FMS server due to the connection speed.

webserver

WEB check server, which can be enabled (1) or disabled (0). It is also known as Goliat server. It has nothing to do with the Web User Experience (WUX) monitoring server.

web_threads

Number of threads assigned to the WEB test server (Goliath). It shows how many simultaneous threads are assigned to this component.

web_timeout

Default expiration time in seconds for web monitoring modules (Goliath).

web_engine

cURL is used by default from version 747 onwards. Set this parameter to LWP to use Library for WWW in Perl (LWP) instead of **cURL** for web monitoring.

inventoryserver

1 enables the Pandora FMS Inventory Server, 0 disables it.

inventory_threads

Number of threads assigned to the remote inventory server.

exportserver

1 enables Pandora FMS Export Server, 0 disables it.

export_threads

Number of threads assigned to the export server. It shows how many simultaneous threads are assigned to this component.

eventserver

E

1 enables Pandora FMS Event correlation Server, 0 disables it (default value is 1).

event_window

E

Event window: It is the time window (in seconds) where the event server will look for events. For example, if set to '3600', the event server will check events generated within the last hour. If you have rules where the time window is longer, you will have to modify this value. A very large value will cause the system to degrade and require more resources (CPU, RAM) to operate.

event_inhibit_alerts

Version NG 7 or superior.

If set to 1, an alert will not be executed (unless it is recovered) if the last event it generated is in 'in progress' status. 0 by default.

icmpserver

E

Enables (1) or disables (0) the Enterprise ICMP server.

The ICMP Enterprise server uses the fping binary binary to perform ICMP requests in bulk. If this component is not enabled, the network server will run the checks, but with a much worse performance.

icmp_threads

Number of threads for the ICMP Enteprise server (default value is 3).

snmpserver

Pandora FMS snmp server enabled (1) or disabled (0).

The SNMP Enterprise server uses the **braa binary** to execute SNMP queries in block. If this component is not enabled, the network server will run the checks.

snmp_threads

Number of threads for Enteprise SNMP server (default value is 3).

transactionalserver

Pandora FMS transactional server enabled (1) or disabled (0).

transactional_threshold

Maximum number of seconds that a Transactional server transaction may take.

prediction_threads

Number of threads for the prediction server.

block_size

Block size for block producer / consumer servers, which is the number of modules per block (the default value is 15). This affects to how requests are processed by SNMP Enterprise and ICMP Enterprise servers.

dataserver_lifo

If enabled (1), XML data files will be processed in a stack instead of a queue, and stale data (i.e., data with a timestamp older than its module's current timestamp) will not trigger events or alerts. Disabled (0) by default.

Incremental modules will lose resolution if XML data files pile up, since newer data will be processed first, causing older data to be discarded.

policy_manager

If active (1), the server listens to the policy queue. By default its value is 1.

event_replication

In case of being active (1) the process of event replication to Metaconsole is performed. This process will not be activated if it is not correctly configured in the console. By default its value is 0.

event_auto_validation

In case of being active (1) new created events autovalidate previous events of the same module. Its value is 1 by default.

event_file

This configuration option allows to specify a text file in which the events generated by Pandora FMS in CSV format will be written. Enabling this option adds a Pandora FMS performance penalty.

For example:

```
event_file /var/log/pandora/pandora_events.txt
```

There is no rotation mechanism for this file, you will have to take it into account since it can grow considerably.

snmp_storm_protection

Pandora FMS's SNMP Console will not process more than this number of SNMP traps from a single source in a defined time interval. If this number is reached, an event is generated.

snmp_storm_timeout

Time interval for snmp_storm_protection in seconds.

E.g. to prevent a single source from sending more than 1000 traps per 10 minutes:

```
snmp_storm_protection 1000
snmp_storm_timeout 600
```

text_going_down_normal

Text for the event that is generated when a module goes into normal status. It supports the `_module_` and `_data_` macros.

text_going_up_critical

Text to be displayed in module events going into critical status. It supports the `_module_` and `_data_` macros.

text_going_up_warning

Text to be displayed in module events going from 'normal' into warning status. It supports the `_module_` and `_data_` macros.

text_going_down_warning

Text to be displayed in module events going from 'critical' into warning status. It supports the `_module_` and `_data_` macros.

text_going_unknown

Text to be displayed in module events going into unknown status. It supports the `_module_` and `_data_` macros.

event_expiry_time

Events older that the specified time (in seconds) will be auto-validated. Set it to `0` to disable this feature.

For example, to automatically validate events 10 hours after they were generated, just use the command:

```
event_expiry_time 36000
```

event_expiry_window

This parameter is used to reduce the impact of 'event_expiry_time' so the entire event table does not have to be searched. Only events more recent than the specified time window (in seconds) will be automatically validated. This value must be higher than event_expiry_time.

The default value is the equivalent of one day:

```
event_expiry_window 86400
```

claim_back_snmp_modules

If set to `1`, SNMP modules run by the Network Server will be claimed back by the SNMP Enterprise Server when the database maintenance script (`pandora_db`) is run.

async_recovery

If set to `1`, asynchronous modules that do not receive data for twice their interval will become normal. Set to `0` to disable.

console_api_url

Console's api direction. Usually, the direction of the server and the console ending with the route `/include/api.php`.

console_api_pass

Password of the console's API. This password can be found in the general section of the setup and can be left empty.

console_user

Console user with permissions to execute API-required actions, like getting a module graph image to add it to an alert email, among others.

For security reasons, it is recommended to use an exclusive user for the API. Such user should not have permission for interactive access to the console, and use of the API should be restricted to only a set of well-known IPs.

console_pass

Password of the API user for the Console.

encryption_passphrase

An encryption phrase used to generate the key for the encrypted password. It is commented by default.

unknown_events

If active (1), events for unknown module status will be enabled. The value set by default is 1.

unknown_interval

Time interval (as a multiple of the module interval) before a module becomes unknown. It equals twice the module's interval by default.

global_alert_timeout

Defines -in seconds- the maximum processing time of an alert. When that time is elapsed, the execution is interrupted. By default, it is 15 seconds. If this token is set to 0, Pandora FMS Server ignores it and alert execution will not be interrupted.

remote_config

This parameter controls whether it is possible to configure the server remotely from the console in the server view. It works by Tentacle in a similar way to the remote configuration of the software agents..

remote_config_address

IP address of the machine where remote configuration files will be sent. It is `localhost` by default.

remote_config_port

Tentacle port for remote configuration. It is 41121 by default.

remote_config_opts

Allows to give additional parameters to the Tentacle client for advanced configurations. They should appear between quotation marks (e.g. “`-v -r 5`”).

warmup_event_interval

In seconds, it specifies the time it will take until status change events are generated again and runs alerts after a server restart.

warmup_unknown_interval

In seconds, it specifies how long it takes for modules to go into unknown status after a server restart.

enc_dir

Path to a directory containing additional .enc files for the XML parser. These files will be automatically loaded by the Data server at startup.

dynamic_updates

Version NG 7 or superior.

The number of times dynamic thresholds will be recalculated per dynamic interval.

dynamic_warning

Version NG 7 or superior.

Percentage relative to the length of the critical interval used to calculate dynamic `warning` thresholds. The lower the value, the closer the `critical` and `warning` thresholds will be.

dynamic_constant

Version NG 7 or superior.

Percentage relative to the module's average used to adjust the module's standard deviation for constant data. A higher value results in wider dynamic threshold intervals.

unknown_updates

Version NG 7 or superior.

Set to `0` by default. If set to `1`, unknown modules will be periodically updated, instead of only once when they become unknown. Alerts associated to unknown modules will be periodically evaluated too.

Setting `unknown_updates` to `1` may affect server performance.

wuxserver

Version NG 7 or superior.

It enables Web User Experience Analysis (WUX) server. It requires configuration of `wux_host` and `wux_port`.

wux_host

Version NG 7 or superior.

It indicates the IP address / FQDN of the server hosting the Pandora Web Robot Daemon service (PWRD).

wux_port

Version NG 7 or superior.

It indicates the port of the Pandora Web Robot Daemon service (PWRD). Its default value is 4444.

wux_webagent_timeout

Version NG 7 or superior.

Maximum time to connect to a destination web address and Selenium server. It is commented by default, with the value 15.

syslogserver

Version NG 7 or superior.

1 enables Pandora FMS **Syslog** Server, `0` disables it.

syslog_file

Full path to **syslog**'s output file. For example: syslog_file /var/log/messages

syslog_threads

Version NG 7 or superior.

Number of threads for the **Syslog** Server.

syslog_max

Version NG 7 or superior.

Maximum number of lines read by the **Syslog** Server on each run.

sync_port

Communication port of the Sync server. It is commented by default, with the value 41121.

sync_ca

CA certificate path to sign certificates to configure SSl communication of the Sync server. It is commented by default, with path `/home/cacert.pem` .

sync_cert

Server certificate path for configuring SSl communication of the Sync server. It is commented by default, with path `/home/tentaclecert.pem` .

sync_key

Private key path of the server certificate for configuring SSl communication of the Sync server. It is commented by default, with the path `/home/tentaclekey.pem` .

sync_retries

Number of attempts to make the connection with the Sync server. It is commented by default, with the value 3 .

sync_timeout

Maximum connection time with the Sync server. It is commented by default, with the value 10 .

sync_address

Address of the Tentacle server for the Sync server.

ha_interval

Execution interval in seconds of Pandora FMS HA Database tool. It is commented by default, with the value 30.

ha_monitoring_interval

Monitoring interval, set in seconds, of the Pandora FMS HA database tool. It is commented by default, with the value 60.

provisioningserver

Version NG 7 or superior.

1 enables Pandora FMS Provisioning Server (Metaconsole), 0 disables it.

provisioningserver_threads

Version NG 7 or superior.

Number of threads for Provisioning Server (Metaconsole).

provisioning_cache_interval

Version NG 7 or superior.

Provisioning Server (Metaconsole) cache refresh interval in seconds (500 by default). The cache contains all the configured Pandora FMS nodes.

ssh_launcher

Version NG 743 or superior.

It indicates the absolute path to the script ssh_launcher.sh that executes remote execution modules. The default path of the script is:

```
/usr/share/pandora_server/util/ssh_launcher.sh
```

Only for el6 in Linux systems.

rcmd_timeout

Version NG 743 or superior.

In seconds, maximum time for the execution of remote execution modules. 10 by default.

This timeout only works to indicate the time that Pandora FMS server will wait to obtain data. The connections will be closed, but the termination of the execution of the command in the remote machine is not assured (this has to be controlled with the command itself).

rcmd_timeout_bin

Version NG 743 or superior.

It indicates the absolute path to the timeout executable for the remote execution modules. It only has effect with the use of ssh_launcher, connections through **plink** from Windows to Linux and connections to Windows® systems.

- In Pandora FMS on **Windows®** the default executable path is:

```
C:\PandoraFMS\Pandora_Server\bin\pandora_exec.exe
```

- In Pandora FMS on **Linux®** the default executable path is:

```
/usr/bin/timeout
```

User and group

Version NG 7 or superior.

From Pandora FMS version 7, it is possible to define in customized installations both the token “user” and the token “group” to indicate which user and group will make the modifications in the console files, such as those related to policies or mass operations or with the `.conf` of the agents located at `/var/spool/pandora/data_in/conf`.

alertserver

Version 757 or later.

```
# Enable (1) or disable (0) Pandora FMS Alert Server.
alertserver 0
```

Enable (`1`) or disable (`0`) **Pandora FMS Alert Server**. Default value: zero.

alertserver_threads

Version 757 or later.

```
# Pandora FMS Alert Server threads.
alertserver_threads 4
```

Pandora FMS **Alert Server** threads. Default value: four.

alertserver_warn

Version 757 or later.

```
# Generate an hourly warning event if alert execution is
# being delayed more than alertserver_warn seconds.
alertserver_warn 180
```

Generate an hourly warning event if alert execution is being delayed more than `alertserver_warn` seconds. Default value: one hundred eigthy seconds.

dbssl

```
dbssl 0
```

Enable (`1`) or disable (`0`) SSL for the database connection. Default value: zero.

See the Security Architecture section **to ensure the operation** of the entire Pandora FMS system.

dbsslcafile

```
# dbsslcafile
```

Path to a file in PEM format that contains a list of trusted SSL certificate authoritiesCertificate_authority. It is commented by default, to enable it you must uncomment and set the path to the file.

See the Security Architecture section **to ensure the operation** of the entire Pandora FMS system.

dbsslcapath

```
# dbsslcapath
```

Path to a directory that contains trusted SSL certificate authority certificates in PEM format. It is commented by default, to enable it you must uncomment and set the path to the file.

See the Security Architecture section **to ensure the operation** of the entire Pandora FMS system.

Environment variables

Pandora FMS' server supports more options than what the configuration file offers. In some particular cases, environmental variables are necessary because the configuration is done on the machine itself. To do this, the server startup script loads the variables of a file in *bash* format which is `/etc/pandora/pandora_server.env` by default.

The variables that can be configured are the following:

PANDORA_RB_PRODUCT_NAME

This variable is required to customize the product name displayed by the server in the initial messages. Otherwise, you would not have access to the custom name until the database was loaded.

PANDORA_RB_COPYRIGHT_NOTICE

This variable is required to customize the author of the product displayed by the server in the initial messages. Otherwise, you would not have access to the custom name until the database was loaded.

Example of an environment variable file

```
#!/bin/bash
PANDORA_RB_PRODUCT_NAME="Custom product"
PANDORA_RB_COPYRIGHT_NOTICE="Custom copyright"
```

SNMPTRAPD configuration

The SNMP Console of Pandora FMS uses **snmptrapd** to receive SNMP traps. **Snmptrapd** is a standard tool, present on almost all UNIX systems, to receive traps and write a logfile. Pandora FMS configures **snmptrapd** to write a custom logfile and reads it every x seconds, executing alerts if defined.

Previously, **snmptrapd** accepted traps by default, without explicitly configuring anything. From version 5.3 onwards, the configuration for access control is more restrictive and it does not allow to receive traps from anyone by default.

If **snmptrapd** runs without a custom configuration, traps are not received and Pandora FMS cannot show them in the console, because the system rejects them.

You are probably required to configure your snmptrapd using the file `/etc/snmp/snmptrapd.conf`. If it does not exist, please check `/var/log/pandora/pandora_snmp.log` file for warnings or errors.

A basic `snmptrapd.conf` could be something similar to this:

authCommunity log public

If does not work on your Linux distribution, please check your **snmptrapd** version syntax to enable trap reception in your **snmptrapd** daemon with the command:

man snmptrapd.conf

Tentacle Configuration

Yo may get more information about **Tentacle protocol** in this section.

By default, Pandora FMS software agents send data packages to the server through Tentacle protocol (Port `41121/tcp` assigned by IANA). The agent could also be reconfigured to send data in alternative ways: local transfer (NFS,SMB),SSH or FTP, etc. If you want them to send data packages using Tentacle protocol, configure a Tentacle server where this data is intended to be received. **By default hen a Pandora FMS server is installed, a Tentacle server is also installed in the same machine by default.**

If it is necessary to adjust some ***parameters of Tentacle server configuration*** , it can be done by modifying the script that launches the Tentacle Server daemon directly, which is at:

```
/etc/init.d/tentacle_serverd
```

Furthermore, there is a list of the different options for Tentacle Server configuration:

;PANDORA_SERVER_PATH: The path to the entry directory of data. The default path is `/var/spool/pandora/data_in`.

TENTACLE_DAEMON: The Tentacle daemon. The default command is `tentacle_server`.

TENTACLE_PATH: The path to the Tentacle binary. The default path is `/usr/bin`.

TENTACLE_USER: User from which the Tentacle daemon will be launched. The default value is `pandora`.

TENTACLE_ADDR: Direction to listen to data packages. If you set 0.0.0.0., it listens to all of them. The default value is to listen in all directions. This is true when its IP is `0.0.0.0`.

TENTACLE_PORT: The listening port for package reception. It is `41121` (official port assigned by IANA) by default.

TENTACLE_EXT_OPTS: Additional options for executing the Tentacle server. You can set up Tentacle to use authentication with certificates and/or symmetric password.

MAX_CONECTIONS: Maximum number of simultaneous connections. The default value is

10.

MAX_SIZE: Maximum file size allowed by the server in bytes. The default value is 2000000.

Pandora Web Robot Daemon (PWRD)

Pandora Web Robot Daemon is a service from Enterprise version that provides the necessary tools to automate web browsing sessions. It is part of the WUX feature. It is available in the module library.

It contains:

- Firefox browser binary version 46.
- Pre-built profile for recording and running web browsing sessions.
- Session Automation Server.
- Web browsing session recorder (.xpi).

For more information related to PWRD, please follow this link.

WEB Console

Pandora FMS web console has a configuration file which is created and configured automatically while it is being installed. Its location is: /consolepath/include/config. php. For example in CentOS systems:

```
/var/www/html/pandora_console/include/config.php
```

Configuration File config.php

The configuration options in the file are included in the header, and these are:

$config[“dbtype”]

Type of database used. It is MySQL by default.

$config[“dbname”]

Database name to connect to. The default value is pandora.

$config[“dbuser”]

Username for the connection to Pandora FMS database. The default value is `pandora`.

$config[“dbpass”]

Password for the connection to Pandora FMS database.

$config[“dbhost”]

IP address or equipment name which hosts the Pandora FMS database. In a reduced installation, it is usually on the same equipment as the server, which is `127.0.0.1` or `localhost`.

$config[“homedir”]

Directory where the Pandora FMS web console is located. This is usually `/var/www/pandora_console` or `/srv/www/htdocs/pandora_console`.

$config[“homeurl”]

Base directory for Pandora FMS. This is usually `/pandora_console`.

$config[“public_url”]

The full URL is set with the string value, the value is the URL inside Pandora FMS Server if you use an inverse proxy e.g. `mod_proxy` from Apache.

Apache server redirection

If you only have one Pandora FMS in your Apache server, then it is possible that you could benefit by automatically redirecting `/pandora_console` when users connect with the `/` URL of their server. To do this, create the following file `index.html` and put it in the web server root directory (`/var/www` or `/srv/www/htdocs`):

```
 <html>
 <head>
 <meta HTTP-EQUIV="REFRESH" content="0;
url=pandora_console/index.php">
 </head>
 </html>
```

Apache Configuration

Pandora FMS has a series of folders with some files that complete its functionality. To

avoid accessing these files, some folders in the console have a `.htaccess` file that restricts access to them. For this to be effective in the Apache configuration, it is necessary to allow these permissions to be overwritten using `htaccess`, for which the token `AllowOverride` must be set to `All`.

```
AllowOverride All
```

instead of:

```
AllowOverride None
```

Go back to Pandora FMS documentation index