Server and console configuration

Server and console configuration

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

Pandora FMS has three essential components that it is essential to configure correctly for a proper functioning:

- Web console.
- PFMS server.
- Database.

This topic explains the configuration files for all three elements, as well as other important elements.

Server

The main configuration of the Pandora FMS server is found in the `pandora_server.conf` file, in the default path `/etc/pandora`.

Elements of the configuration file

servername

By default it is stored as a comment and the name of the machine is used by the operating system.

Changing the name once it's working could cause remote checks to stop working, as you would have to reconfigure the default server on all existing agents to use the new server, as well as remove the server name from the server list ancient.

incomingdir

Input directory for XML data packages, by default at:

```
/var/spool/pandora/data_in/
```

log_file

Record file (log), by default at:

```
/var/log/pandora/pandora_server.log
```

snmp_logfile

SNMP console log by default at:

```
  /var/log/pandora/pandora_snmptrap.log
```

errorlog_file

Default error log:

```
/var/log/pandora/pandora_server.error
```

daemon

It runs in daemon mode (background), yes `1`; if it is `0` it runs in the foreground. Commented out by default. It can also be configured on the command line with the `-D` option.

dbengine

Database to use, by default MySQL.

```
# dbengine:mysql
dbengine mysql
```

dbname

Name of the database to which the server will connect. By default it is `pandora`.

dbuser

Username for connection to the database. Default is `pandora`.

dbpass

Password for the connection to Pandora FMS database.

dbhost

IP address, URL or name of the computer that hosts Pandora FMS database. In small installations it is usually the same computer where the server is, that is to say `127.0.0.1`.

dbport

TCP port where the database engine listens, by default `3306` is used.

verbosity

Detail level for server logs, from 0 (disabled) to 10 (maximum level of detail).

The continuous use of high values is not recommended due to the growth spike of log files, which may cause performance issues in the system.

master

Primary server priority. The server with the highest value (positive integer numeric value) running will be the master. Ties are broken randomly. If set to 0, this server will never become principal.

snmpconsole

When activated (with value 1) it indicates that the SNMP trap reception console is activated in the configuration. Value `0` disables it.

snmpconsole_threads

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

snmpconsole_lock

If set to `1`, traps from the same source will never be processed at the same time. Set to `0` by default.

snmpconsole_threshold

The time between consecutive reads of the SNMP log file in seconds. The default value is `server_threshold`.

translate_variable_bindings

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

translate_enterprise_strings

E When set to value `1` (which is the default value), the SNMP console will try to translate enterprise strings when processing SNMP traps.

snmp_ignore_authfailure

The snmptrapd service will ignore `authenticationFailure` SNMP traps if it is set to `1` (which is the default value).

snmp_pdu_address

If enabled (value `1`), the snmptrapd service will read from the Protocol data units (PDU) address instead of the Agent address. By default its value is `0`.

snmp_trapd

Path to the `snmp_trapd` binary file. If it is manual, the server will not start the `snmp_trapd`. By default its value is manual.

snmp_forward_trap

It enables (1) or disables (0) tSNMP trap forwarding to the host indicated in snmp_forward_ip

snmp_forward_ip

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

Be especially careful not to enter a forwarding address to
the Pandora FMS server itself, as this would create a
forwarding loop and could collapse the monitoring server.

snmp_forward_version

SNMP version to be used to send SNMP traps, one of the following values:1, 2c or 3.

snmp_forward_secName

It specifies the security name for SNMP version 3 authentication.

snmp_forward_engineid

It specifies the authorized Engine ID of SNMP version 3.

snmp_forward_authProtocol

It specifies the SNMP version 3 authentication protocol: MD5 or SHA.

snmp_forward_authPassword

It specifies the SNMP version 3 authentication password

snmp_forward_privProtocol

It specifies the privacy protocol of SNMP version 3: DES or AES.

snmp_forward_privPassword

It specifies the privacy password for SNMP version 3.

snmp_forward_secLevel

Exclusive to SNMP version 3. It specifies the security level. This parameter can take only the following values:

- `noAuthNoPriv`.
- `authNoPriv`.
- `authPriv`.

snmp_forward_community

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

networkserver

Pandora FMS Network Server: activated `1` or deactivated `0`.

dataserver

Pandora FMS Data Server: activated `1` or deactivated `0`.

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

dataserver_smart_queue

Version 765 or later.

```
# Enable (1) or disable (0) the Data Server smart queue, which gives priority
# to new data coming from agents at the expense of buffered XML files.
dataserver_smart_queue 1
```

When activated (1), the server gives priority to new data arriving from each agent, ahead of less recent data (LIFO mode).

pluginserver

Pandora FMS remote plugin server: activated 1 or deactivated 0.

plugin_exec

It indicates the absolute path to the program that runs the plugins in a time-controlled manner, by default:

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

If the base system does not have this command, you must use instead `/usr/bin/pandora_exec`, which is included with Pandora FMS.

predictionserver

Pandora FMS prediction server: activated 1 or deactivated 0.

wmiserver

Pandora FMS WMI server: activated 1 or deactivated 0.

wmi_client

```
# WMI client binary (wmic by default).
wmi_client pandorawmic
```

Full path <path> to pandorawmic, default

```
/usr/bin/pandorawmic
```

syncserver

```
# SyncServer
#syncserver
```

Pandora FMS Synchronization server (Sync Server) : activated 1 or deactivated 0.

network_timeout

In seconds, expiration time or timeout for ICMP checks. By default its value is 2 seconds. If you are going to perform checks on WAN networks, it is advisable to increase this value to avoid false positives as some checks may require more time.

The more timeout you set, the more time it will take to run the checks. Always look for a studied and adequate value.

server_keepalive

Time before declaring the server down in seconds. Each server checks the status of the servers around it, and if the last update date of one of them exceeds this value, it will report it as offline. This affects, in the case of having several servers, how High Availability (HA) works.

It is essential that in the case of having several servers, all their internal times are synchronized through NTP.

thread_log

Set by default to `0`, unless Pandora FMS server is being debugged. Value `1` causes the server threads to periodically dump their state to a disk at the following location:

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

server_threshold

The number of seconds in the main loop, in seconds. By default its value is 5.

This is a very important value for server configuration, since it defines how many times Pandora FMS will search to see if there is pending data in the database or in the hard disk (XML file search). 5 to 15 is a valid value for most occasions. If it is set to 1, CPU consumption will increase by a lot. Value 1 can be used for special occasions, such as when, for example, Pandora FMS has been in downtime for some time and there are many XML files and network tasks yet to be processed. It can be set to 1 and it will process

pending tasks a little faster, but when once it is done, it should be set to between 5 and 15.

With very low values and high load, there is an "overheating" effect that causes the CPU and memory consumption of the server to progressively increase.

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

network_threads

Number of threads for the Network Server. It indicates how many checks can be performed simultaneously. Deliberately increasing this value is not recommended as it may cause excessive consumption of server resources. A number higher than twenty threads requires to have a machine with many processors or independent cores.

icmp_checks

It defines the number of pings for each `icmp_proc` module. At least one of those checks must return 1 for the Module to be taken as correct. Its default value is 1. If a higher number is entered and the first ping is successful, the rest are not performed.

In the case of having networks that have limited reliability, it is recommended to set 2 or 3. A higher number will cause a significant decrease in check rate per second.

Not to be mistaken with the `icmp_packets` parameter, which refers to the number of packets within the ping action itself. Value `icmp_checks` defines the number of pings, each with its own `icmp_packets`.

icmp_packets

It defines the number of packets that are sent in each ping request. Default value: 1.

tcp_checks

Number of TCP retries if the first one fails. The predetermined value is 1.

tcp_timeout

Specific timeout for TCP checks. The default value is 30 seconds.

A high number (greater than 40) will cause the check rate per second to drop significantly in the event of a network segment failure.

snmp_checks

Number of SNMP retries if the first one fails. The predetermined value is 1.

snmp_timeout

Specific timeout for SNMP checks. The default velue is 3 seconds.

A high number will cause a significant decrease in check rate per second in the event of a network segment failure.

snmp_proc_deadresponse

It returns DOWN if a boolean SNMP module (proc) cannot be contacted or if it receives NULL. If set to 0, it is ignored.

plugin_threads

Number of threads for the remote plugin server. It indicates how many checks can be performed simultaneously.

plugin_timeout

Expiration time, in seconds, of checks with remote plugins. After this time, the Module status will be shown as unknown. Its default value is 5, although you may probably want to raise it to a higher value, in case you have plugins that might take longer than that.

wmi_timeout

WMI check expiration time. After that time, the Module status will be shown as unknown. Its default value is 10 seconds.

wmi_threads

Number of threads for the WMI server. It indicates how many checks can be performed simultaneously.

recon_threads

Number of threads for the network recognition server. It indicates how manyChecks can be performed simultaneously.

dataserver_threads

Number of threads for the Data Server. It indicates how many XML files can be processed at the same time. As a specific rule for the Data server, a number of threads higher than the number of physical processors the machine has should not be used.

Depending on the number of XML the server must process, a normal value ranges from 1 to 4. For environments with a huge load, the value can go up, but up to the maximum number of CPU's that the server has, never exceeding it. In any case, a value greater than 10 does not usually impact performance, but it does impact server memory consumption.

mta_address

IP address of the email server (Mail Transfer Agent).

Make sure that your Pandora FMS server is able to resolve the mail server in charge of your email domain through your DNS server.

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

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

If it is not specified, Pandora FMS Console confiduration will be used. It is possible to have a different MTA configuration for Pandora FMS server and Pandora FMS Console.

mta_port

Email server port. By default port 25.

mta_user

Username for the email server (if required).

mta_pass

Password for the email server (if required).

mta_auth

Email server authentication system, if necessary. Valid values are:

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

mta_from

Email address from which emails will be sent. By default it is `pandora@localhost`.

mta_encryption

Encryption type of the SMTP connection (`none`, `ssl`, `starttls`).

mail_in_separate

If set to `1`, mail delivery will be separate for each recipient. If set to `0`, the mail will be shared among all recipients. By default, `1`.

xprobe2

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

nmap

Required for the Discovery server. By default it is located at `/usr/bin/nmap`.

fping

Required for the Network Server and the Enterprise ICMP Network Server. By default it is located at `/usr/sbin/fping`.

nmap_timing_template

A value specifying the depth of the nmap scan, on a scale of 1 to 5. 1 means slower but more reliable, 5 means faster but less reliable; 2 is the default value.

recon_timing_template

Just like nmap_timing_template, but applied to Satellite server and Discovery server network scans.

snmpget

It is required for SNMP checks. By default it is at `/usr/bin/snmpget`. It refers to the location of the system's standard SNMP client. In the case of MS Windows®, a binary is provided for this purpose.

braa

Location of the braa binary, used by the Enterprise SNMP server (`/usr/bin/braa` by default).

braa_retries

Number of retries before braa passes the Module to the Network Server on error.

fsnmp

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 the new Agents automatically created through data file reception. If there is no group defined here, the Agents will be created in the group that contains the XML.

autocreate_group_name

Name of the default group for the new Agents created automatically through data file reception. If there is no group defined here, the Agents will be created in the group that contains the XML.

```
# Works like autocreate_group, except the name of the group is specified
(instead of its id).
# Do not set both.
#autocreate_group_name Unknown
```

It works like autocreate_group, except that the name of the group (rather than its ID) is specified. Do not set both.

autocreate_group_force

If set to value `1`, new Agents will be added to the group specified by autocreate_group (the group specified by the Agent will be used as a last resort) .

If set to the value `0`, new Agents will be added to the group specified by the agent (the group specified by autocreate_group will be used as a last resort).

autocreate

If set to `1`, Agents will be autocreated when data files are received with an Agent ID that does not

exist in the system.

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

max_log_size

Maximum size of Pandora FMS log file, in bytes. When this size is reached, the file will be renamed as `pandora_server.log.old` and the server will generate one with the original name, `pandora_server.log`. The default size is 65,536 bytes.

max_log_generation

It specifies the maximum number of Pandora FMS log files (minimum 1, maximum 9). The predetermined value is 1.

max_queue_files

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

Incremental modules may not work correctly if this value is not large enough to contain all XML data files.

use_xml_timestamp

By default it is activated (`1`) and uses the date and time (timestamp) defined within the XML (`.data`), that is, the timestamp generated by the agent.

If disabled (`0`), the timestamp from the XML file will be used, i.e. the server s timestamp. This disables globally the use of the dates generated by the Agents and uses the date and time of the server as a reference for all data, since this timestamp is generated at the moment that Pandora FMS server receives the XML.

This operation changed in version 747 of Pandora FMS. In previous versions this token is disabled by default.

There is a similar feature at the Agent level, so that the agent data is evaluated with the receipt date of the file.

auto_restart

Disabled by default. If enabled (value in seconds), it forces the server to do an internal reboot every X number of seconds (1 day = 86400). This option is useful if you observe degradation due to the uncontrolled crash of a specific Pandora FMS thread or server.

restart

Disabled by default (`0`). On a critical error, the server will restart after a given number of seconds.

If you use pandora_ha, it is recommended to set this value to zero and let HA do the rebooting when needed.

restart_delay

```
# Pandora FMS will autorestart itself each XXX seconds, use this if you
experience problems with
# shutting down threads, or other stability problems.

# auto_restart 86400

# Pandora FMS will restart after restart_delay seconds on critical errors.

reset 1
restart_delay 60
```

By default `60`. If restart is enabled, that is the number of seconds the server will wait before restarting after a critical error.

activate_gis

To activate (`1`) or deactivate (`0`) server GIS features.

location_error

Error margin o(in meters) to consider two GIS locations as the same location.

recon_reverse_geolocation_file

File with information on reverse geolocation. This file must have format MaxMind GPL `GeoLiteCity.dat`. If this option is commented out in the configuration file, IP geolocation will be disabled when creating Agents through recon and Software Agents. Neither will geolocation be carried out if GIS functionalities are generally deactivated (activate_gis).

recon_location_scatter_radius

Radius (in meters) for the “circle” within which Agents discovered by a network task will be located. The center of the circle will try to be calculated based on geolocating the discovered IP address.

self_monitoring

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

self_monitoring_interval

Time interval, in seconds, for self_monitoring. Default value: 300 seconds.

update_parent

It defines whether the Agent can update its parent by sending the name of the parent in the XML, but if the parameter is undefined or 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 will look for an Agent with this name, and if found, it updates the Agent's parent from the XML.

google_maps_description

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

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

openstreetmaps_description

This activates the conversion of GPS coordinates into a textual description of the address (reverse geolocation). For that, the API of OpenStreetMaps will be used. This service is not as accurate as Google Maps, but it is free. It also has the advantage that it can, through some code modifications, be used to connect to a local server.

If it is used with a direct Internet connection (by default), its performance for processing GIS information may become poorer due to the connection speed to the OpenStreetMaps API from Pandora FMS server.

webserver

Pandora FMS WEB checks server: activated `1` or deactivated `0`.

web_threads

It indicates how many simultaneous threads are allocated to the `webserver` component.

web_timeout

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

web_engine

As of version 747, cURL is used by default. Set LWP to use Library for WWW in Perl (LWP) instead of

cURL for web monitoring.

inventoryserver

Pandora FMS remote inventory server: activated `1` or deactivated `0`.

inventory_threads

Number of threads allocated to the remote inventory server.

exportserver

Pandora FMS export server: activated `1` or deactivated `0`.

export_threads

Number of threads assigned to the export server. It indicates how many concurrent threads are allocated to this component.

eventserver

Pandora FMS event alert and correlation alert server: activated `1` or deactivated `0`. See also correlationserver .

```
# Enable (1) or disable (0) Pandora FMS Event Server (PANDORA FMS ENTERPRISE
ONLY).
eventserver 0
```

event_window

This is the time frame within which the Event Correlation Server will take events into account.

event_inhibit_alerts

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

icmpserver

Pandora FMS Enterprise ICMP server: activated 1 or deactivated 0.

The ICMP Enterprise Server uses the fping binary to make bulk ICMP requests. If this component is not enabled, the Network Server will execute the checks, but with poorer performance.

icmp_threads

Number of ICMP Enterprise Server threads (3 by default).

snmpserver

Pandora FMS Enterprise SNMP server: activated 1 or deactivated 0.

The Enterprise SNMP server uses the braa binary to execute bulk SNMP requests. If this component is not enabled, the Network Server will execute the checks.

snmp_threads

Number of Enterprise SNMP server threads (3 by default).

prediction_threads

Number of threads for the Prediction Server.

block_size

Block size of block producer/consumer servers, i.e. number of modules per block (15 by default). This affects how it processes requests to the Enterprise SNMP Server and the Enterprise ICMP Server.

dataserver_lifo

If on (1), XML data files will be processed on a stack instead of a queue, and old data (for example, data with a timestamp older than the timestamp of your module) will not trigger events or alerts. Disabled, value (0) by default.

Incremental Modules will lose resolution if XML data files accumulate, since new data will be processed first, causing old data to be discarded.

policy_manager

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

event_auto_validation

If it is active (1), the new events created self-validate previous events of the same module. By default its value is 1.

event_file

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

For example:

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

There is no rotation mechanism for this file, you will need
to be aware of this as it can grow very large.

snmp_storm_protection

```
# Set the maximum number of traps that will be processed
# from a single source in a configured time interval.
snmp_storm_protection 25
```

SNMP trap storm protection system by which Pandora FMS 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_silence_period

```
# Silenced time period in seconds, when trap storm is detected
snmp_storm_silence_period 300
```

When detecting a SNMP trap storm, it will go into a silence period (in seconds) set by this parameter. Default value: `300`.

snmp_storm_timeout

Timeout interval for snmp_storm_protection in seconds.

For example, to prevent a single source from sending more than 1000 SNMP traps every 10 minutes:

```
   snmp_storm_protection 1000
   snmp_storm_timeout 600
```

text_going_down_normal

Text displayed on module events going into normal state. It supports `_module_` and `_data_` macros.

text_going_up_critical

Text displayed on module events going into critical state. It supports `_module_` and `_data_` macros.

text_going_up_warning

Text displayed on module events going into warning state from normal state. It supports `_module_` and `_data_` macros.

text_going_down_warning

Text displayed on events of modules going into warning state from critical state. It supports `_module_` and `_data_` macros.

text_going_unknown

Text displayed on module events going into unknown state. It supports `_module_` and `_data_` macros.

event_expiry_time

Events older than the time specified in `event_expiry_time` (number of seconds) will be validated automatically. To disable this feature set the value to zero (`0`).

event_expiry_window

This parameter is used to reduce the impact of event_expiry_time so that the entire event table does not have to be checked. Only events newer than the specified time window (in seconds) will auto-validate. This value must be higher than event_expiry_time.

The default is one day:

```
event_expiry_window 86400
```

claim_back_snmp_modules

E

If set to 1, the SNMP modules running on the network Server will be returned to the Enterprise SNMP Server when the database maintenance script (`pandora_db`) is executed.

async_recovery

If it is set to 1, asynchronous modules that do not receive data for twice their interval will go into normal state. Set to 0 to disable it.

console_api_url

Console API address. Normally the address of the Server and the Console end with the path `/include/api.php`.

console_api_pass

Console API password. This password is found in the general section of the Console configuration and can be empty.

console_user

Console user with permissions to perform the actions required by the API, such as obtaining a graph from a module to insert into an alert email, among other actions.

For security reasons, it is recommended to use an exclusive user for the use of the API. Said user must not have permission to interactively access the Console, and the use of the API must be restricted to only a set of well-known IP addresses.

console_pass

Password of the API user for the Console.

encryption_passphrase

Encryption phrase used to generate the key for the encrypted password. It is commented out by default.

unknown_events

If it is active (1), module events in unknown state are enabled. The default value is 1.

unknown_interval

The time interval (as a multiple of the Module interval) before the Module goes into unknown state. It is equal to twice the default Module interval.

global_alert_timeout

It indicates, in seconds, the maximum time that an alert can be processed. After that time, the execution is interrupted. By default it has a value of 15 seconds. In order for Pandora FMS Server to ignore this timeout and never end the execution of the alert prematurely, set this parameter to `0`.

remote_config

This parameter controls whether it is possible to configure Pandora FMS server remotely from the Console in the servers view, `0` disabled, `1` enabled (then you must restart PFMS server). It works by Tentacle in a similar way to the remote configuration of the Software Agent.

remote_config_address

IP address of the machine where you want to send the remote configuration. By default it is `localhost`.

remote_config_port

tentacle protocol port for remote configuration. By default 41121 is used.

tentacle_service_watchdog

Version 762 or later.

It enables or disables the watchdog for the Tentacle server. Default value 1 (enabled), `0` to disable.

See also “Manual start and stop of Pandora FMS servers”.

```
# Enable (1) or disable (0) the Tentacle Server watchdog (enabled by default).
tentacle_service_watchdog 1
```

remote_config_opts

It allows passing additional parameters to the Tentacle client for advanced configurations. They must be enclosed in quotes (for example, “`-v -r 5`”)

warmup_event_interval

It specifies the time, in seconds, before state change events are regenerated and alerts run after a server restart.

warmup_unknown_interval

It specifies the time, in seconds, before Modules can go into unknown state after a server restart.

enc_dir

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

dynamic_updates

The number of times dynamic thresholds are recalculated per dynamic interval.

dynamic_warning

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

dynamic_constant

Percentage related to the average of a Module that is used to adjust the standard deviation of a Module when the data are constant. A higher value results in wider dynamic ranges.

unknown_updates

If set to 1, Unknown Modules will be checked periodically instead of once when they go unknown. Alerts associated with unknown modules will also be evaluated periodically. 0 is the default value.

Using unknown_updates on 1 may affect server performance.

wuxserver

It enables the analysis server of web user experience (WUX). It requires wux_host and wux_port to be configured.

wux_host

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

wux_port

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

wux_webagent_timeout

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

wux_timeout

Maximum time of WUX transactions. Default value thirty 30.

clean_wux_sessions

```
# Force closing previous sessions on remote wux_host,
# only for Selenium Grid server 3.
#clean_wux_sessions 1
```

If this parameter is activated (1) it allows cleaning the WUX seesion that may be queued every time Pandora FMS server starts (only for Selenium 3) .

syslogserver

Pandora FMS syslog server: enabled 1 or disabled 0.

syslog_file

Absolute path of the syslog output file. For example:

```
syslog_file /var/log/messages
```

syslog_threads

Number of threads for the syslog server.

syslog_max

Maximum number of lines read by the syslog server on each run.

sync_port

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

sync_ca

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

sync_cert

Server certificate path to configure SSL communication of Sync server. It is commented out by default, with path `/home/tentaclecert.pem`.

sync_key

Path of the private key of the server certificate to configure SSL communication of Sync server. It is commented out by default, with path `/home/tentaclekey.pem`.

sync_retries

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

sync_timeout

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

sync_address

Tentacle server address for the Sync server.

ha_interval

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

ha_monitoring_interval

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

provisioning server

Set to 1, it enables the Provisioning Server (Metaconsole) of Pandora FMS, 0 disables it.

provisioningserver_threads

Number of threads of the Provisioning Server (Metaconsole) of Pandora FMS.

provisioning_cache_interval

Pandora FMS 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 higher.

It indicates the absolute path to the `ssh_launcher.sh` script that runs the remote launch modules. The default path of the script is:

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

Only for EL6 (Enterprise Linux 6).

rcmd_timeout

Version NG 743 or higher.

In seconds, maximum time for the execution of remote execution modules. By default its value is 10.

This timeout only takes effect to indicate the time that

Pandora FMS server will wait to obtain data. The connections will be terminated but the completion of the command execution on the remote machine is not ensured (it must be controlled by the command itself).

rcmd_timeout_bin

Version NG 743 or higher.

It indicates the absolute path to the timeout executable for Remote Execution Modules. It only takes effect with the use of ''ssh_launcher'', connections via plink from Windows® to Linux, and connections to Windows® systems.

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

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

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

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

user and group

In customized installations, both the “user” token and the “group” token can be defined to indicate which user and group will carry out the modifications in the Console files, such as those related to policies, massive operations or with the `.conf` of the agents located at `/var/spool/pandora/data_in/conf`.

alertserver

Version 756 or later.

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

Enable (`1`) or disable (`0`) the Alert Server. Default value: zero.

alertserver_threads

Version 756 or later.

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

Number of threads to be handled by the Alert Server. Default value: four.

alertserver_warn

Version 756 or later.

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

Maximum number of seconds that the execution of the Alert Server can be delayed. If you exceed this limit, an alert event will be generated every hour. Default value: one hundred and eighty seconds.

dbssl

```
dbssl 0
```

It enables (`1`) or disables (`0`) the use of SSL for the connection to the database. Default value: zero.

dbsslcafile

```
# dbsslcafile
```

Path or location of the file, in PEM format, that contains a list of SSL certificates issued by a Certificate Authority. It is commented by default, to enable it uncomment it and set the path to the file.

dbsslcapath

```
# dbsslcapath
```

Path or location of the directory or folder that houses SSL certificates issued by a Certificate Authority. Certificates must be in PEM format. It is commented by default, to enable it you must uncomment it and set the path to the directory.

verify_mysql_ssl_cert

Version 766 or later.

```
verify_mysql_ssl_cert 0
```

If it is set to 1, it performs the verification in the MySQL connection (CN of the SSL certificate), if they do not match, it does not connect. Default value 0.

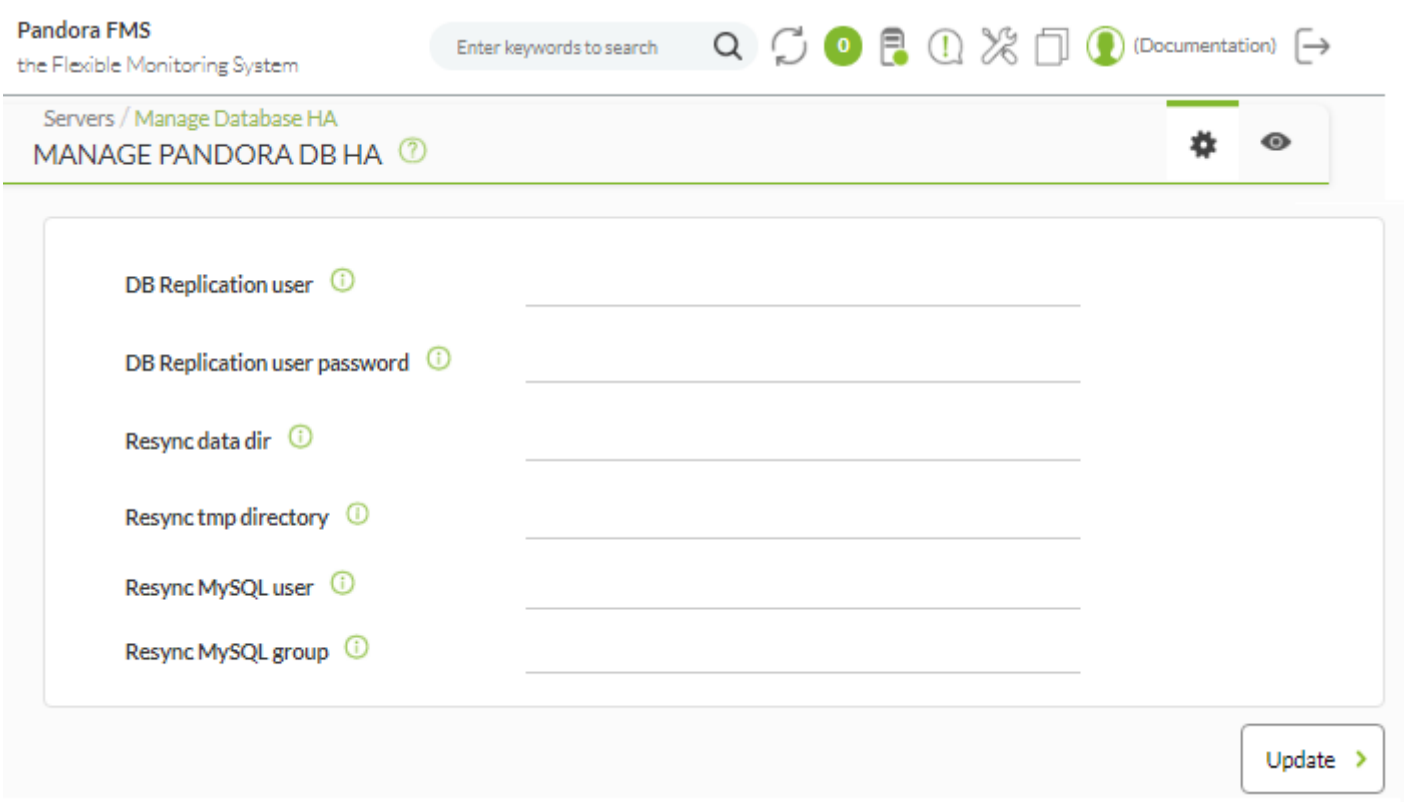
splitbrain_autofix

```
# Pandora FMS HA MySQL cluster splitbrain auto-recovery
# (PANDORA FMS ENTERPRISE ONLY)
#IMPORTANT! Please understand and configure all settings from
#
pandora_console/index.php?sec=gservers&sec2=enterprise/godmode/servers/HA_cluste
r&tab=setup
# before enable this feature.
#splitbrain_autofix 0
```

E It is a parameter (enabled with 1) that allows automatically recovering pandora_ha environments in which Splitbrain was produced, that is, that both nodes behave as principal or Master.

Consult section "High availability in the database" to ensure the operation of HA Pandora FMS.

You must understand and configure all the values from Servers → Manage database HA → Setup:



See section "Automatic node recovery in Splitbrain" for more details.

ha_max_splitbrain_retries

```
# Pandora FMS HA MySQL cluster splitbrain auto-recovery settings
# (PANDORA FMS ENTERPRISE ONLY)
# Maximum number of retries
#ha_max_splitbrain_retries 2
```

(E) Number of times to perform autorecovery on failure the first time of the function Splitbrain autofix.

See the section "Automatic node recovery in Splitbrain" for more details.

ha_max_resync_wait_retries

```
# Pandora FMS HA MySQL cluster splitbrain auto-recovery settings (PANDORA FMS
ENTERPRISE ONLY)
# Maximum number of retries to verify resync status.
#ha_max_resync_wait_retries 3
```

(E) Number of times synchronization is checked for success at the end of the function process

Splitbrain autofix.

See the section "Automatic node recovery in Splitbrain" for more details.

ha_resync_sleep

```
# Pandora FMS HA MySQL cluster splitbrain auto-recovery settings (PANDORA FMS
ENTERPRISE ONLY)
# Maximum number of seconds waiting while verifying resync status.
#ha_resync_sleep 10
```

E Seconds that will elapse between each of the retries or retries configured in the token previous ; both parameters belong to the function Splitbrain autofix.

See section "Automatic node recovery in Splitbrain" for more details.

ncmserver

```
# Network manager configuration server (PANDORA FMS ENTERPRISE ONLY).
ncmserver 1
```

E NCM Server. With this configuration parameter you will activate the network device configuration management server. On: `1` , off `0`. By default it is disabled.

ncmserver_threads

```
# Threads for NCM server (PANDORA FMS ENTERPRISE ONLY).
ncmserver_threads 1
```

E Number of threads of the NCM server.

ncm_ssh_utility

```
# NCM utility to execute SSH and Telnet connections.
ncm_ssh_utility /usr/share/pandora_server/util/ncm_ssh_extension
```

E Path where the execution binary of the NCM server is located. By default it is installed on: `/usr/share/pandora_server/util/ncm_ssh_extension`

This binary is used to connect via Telnet or SSH to network devices configured within the NCM server.

correlationserver

```
# Enable (1) or disable (0) Pandora FMS Correlation Server
# (PANDORA FMS ENTERPRISE ONLY).
correlationserver 0
```

E This server replaces eventserver. To use it, it will be necessary to deactivate the `eventserver` and activate the `correlationserver` in this way:

```
event server 0
correlationserver 1
```

This server evaluates correlated alerts at time intervals, optimizing the work queue in environments with many simultaneous events.

The pass and drop methods of alerts have no effect when enabled (they always evaluate to pass). The evaluation of the event pools and logs is done every threshold defined in correlationtion_threshold.

This server incorporates a correlated alert recovery system as long as there are no events or logs in the evaluation pool that meet any alert rule. When the alert is recovered, the action is automatically launched with the 'recovery' conditions defined in the action. There are no macros since the trigger is caused by the absence of information, so the only thing that is reported in the recovery is the title of the recovered alert and the time of its recovery.

correlation_threshold

```
# Time in seconds to re-evaluate correlation alerts pool
# (PANDORA FMS ENTERPRISE ONLY).
correlation_threshold 30
```

E Time, in seconds, to evaluate the event pools and logs for the correlationserver.

preload_windows

```
# Pre-load windows on start with available information.
# (PANDORA FMS ENTERPRISE ONLY).
#preload_windows 0
```

E

When Pandora FMS server starts, it preloads the events within the event_window, to evaluate correlated alerts. With the correlationserver, if this option is disabled, restarting the server will trigger a recovery for each alert that was triggered. It is recommended to have it enabled so that recoveries are not launched at each reboot.

discoveryserver

```
# Activate (1) Pandora FMS Discovery server
discoveryserver 1
```

With this configuration parameter you activate the Discovery Server. On: 1 , off 0. By default it is activated.

elastic_query_size

```
# Log retrieving, items per request.
elastic_query_size 10
```

Items per request for log collection (logs) with Elasticsearch. Higher values may stop Elasticsearch. Default value: ten 10.

event_server_cache_ttl

```
# Correlated Alerts, group cache ttl (in seconds). Set to 0 to disable.
# (PANDORA FMS ENTERPRISE ONLY).
#event_server_cache_ttl 10
```

E It sets, for the correlationserver, the time to live (in seconds) for the group cache. Default value when enabled: ten 10.

log_window

```
# Correlated Alerts, log window in seconds (3600 by default)
# (PANDORA FMS ENTERPRISE ONLY).
log_window 3600
```

E It sets, for the correlationserver, the time period (in seconds) for the record or log. Default value: 3600. See also event_window.

unknown_block_size

Version 769 or later.

```
# Number of unknown modules that will be processed per iteration.
unknown_block_size 1000
```

Number of unknown modules to be processed in PFMS data server, per iteration (`1000` by default).

netflowserver

Version 770 or later.

Activate (`1`) or disable (`0`) Pandora FMS Server NetFlow.

```
# Enable (1) or disable (0) the Pandora FMS Netflow Server (PANDORA FMS
ENTERPRISE ONLY).
netflowserver 0
```

netflowserver_threads

Version 770 or later.

Number of threads for Pandora FMS NetFlow server.

```
# Number of threads for the Pandora FMS NetFlow Server (PANDORA FMS ENTERPRISE
ONLY).
netflowserver_threads 1
```

syslog_whitelist

When activating the [[:en:documentation:pandorafms:installation:04_configuration#syslogserver|Syslog server]] , sets the allowed logs using regular expression filtering (regexp).

```
# Whitelist regexp filter for the Syslog Server (PANDORA FMS ENTERPRISE ONLY).
# syslog_whitelist .*
```

With `.*` everything is allowed; see “PFMS server level filters” for more details.

syslog_blacklist

When activating the [[:en:documentation:pandorafms:installation:04_configuration#syslogserver|Syslog server]] , sets locked logs using regular expression filtering (regexp).

```
# Blacklist regexp filter for the Syslog Server (PANDORA FMS ENTERPRISE ONLY).
# syslog_blacklist regex
```

See “PFMS server level filters” for more details.

Environment Variables

Pandora FMS server supports some more options than those offered by the configuration file. In particular cases, environment variables are necessary since the configuration is done on the machine itself. To do this, the server startup script loads the variables from a file in BASH format which, by default, is:

```
/etc/pandora/pandora_server.env
```

The variables that can be configured are the following:

PANDORA_RB_PRODUCT_NAME

This variable is needed to customize the product name in the initial messages displayed by the server. Otherwise, the custom name would not be accessible until the database was loaded.

PANDORA_RB_COPYRIGHT_NOTICE

To customize the author of the product in the initial messages displayed by the server, this variable is necessary. Otherwise, the custom name would not be accessible until the database was loaded.

Environment variable file example

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

SNMPTRAPD Configuration

Pandora FMS SNMP Console uses snmptrapd to receive SNMP traps. The snmptrapd service is a standard tool, present on almost all UNIX systems, for receiving SNMP traps and writing a log file. Pandora FMS configures snmptrapd to write a custom log file and reads it every x number of seconds.

Previously, snmptrapd accepted SNMP traps by default, without explicitly configuring anything. As of version 5.3, the access control configuration is more restrictive and by default does not allow receiving SNMP traps from anyone.

If snmptrapd is executed without a custom configuration, SNMP traps are not received and Pandora FMS cannot show them in the Console, because the system rejects them.

Most likely you will need to configure the file:

```
/etc/snmp/snmptrapd.conf
```

If the above file does not exist, to debug check the following file:

```
/var/log/pandora/pandora_snmp.log
```

A basic configuration of the `snmptrapd.conf` file would be the following:

```
authCommunity log public
```

If it does not work on your Linux distribution, please check your system version snmptrapd syntax to allow receiving traps in the snmptrapd daemon with the command:

```
man snmptrapd.conf
```

Tentacle Configuration

You may learn more about the Tentacle protocol in this section.

Pandora FMS Software Agents by default send the data packets to the server through the Tentacle protocol (port `41121/tcp` assigned by IANA). You may also reconfigure the Software Agent to send data in alternative ways: local (NFS, SMB) or remote (SSH, FTP, etc.) transfers. If you want them to send the data packets through the Tentacle protocol, you must set up a Tentacle server that will receive that data. By default when installing Pandora FMS server, a Tentacle server is installed on the same machine.

If it is necessary to adjust some Tentacle server configuration parameters you may directly modify the Tentacle Server daemon launcher script located at:

```
/etc/init.d/tentacle_server
```

The different Tentacle Server configuration options are listed below:

PANDORA_SERVER_PATH

Path to the data input directory. By default it is:

```
/var/spool/pandora/data_in
```

TENTACLE_DAEMON

Tentacle daemon. By default it is `tentacle_server`.

TENTACLE_PATH

Path to the Tentacle binary. By default it is:

```
  /usr/bin
```

TENTACLE_USER

User with which the Tentacle daemon will be launched. By default it is `pandora`.

TENTACLE_ADDR

Address from which to listen for data packets. By default it listens on all addresses, that is, its value is `0.0.0.0`.

TENTACLE_PORT

Listening port for packet reception. By default it is 41121.

TENTACLE_EXT_OPTS

Additional options with which to run the Tentacle server. Here you may configure Tentacle to use authentication with symmetric password or certificates.

MAX_CONNECTIONS

Maximum number of simultaneous connections that can be made. Default value

`10`.

MAX_SIZE

Maximum size of the file that can be processed in bytes. Default value `2000000`.

See also:

- Tentacle secure configuration.
- Data compression in Tentacle.

Pandora Web Robot Daemon (PWRD)

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

It contains:

- Mozilla Firefox® version 46 browser binary.
- Prebuilt profile for recording and executing web browsing sessions.
- Session automation server.
- Web browsing session recorder (`.xpi`)

For more information about PWRD, please access the following link.

Server multithreading configuration

Version 770 or later:

For large environments with more than 50,000 modules,
both local (`dataserver`) and remote.

If you have a machine with a large number of cores and RAM memory, it is convenient to separate the processes for the most demanding servers (such as the Dataserver), using this option.

This will make it possible to make optimal resource use, without affecting the tasks of the main server, delegating the most aggressive workload to a secondary process(es) without affecting the operation of the rest of the components that are managed by the main process.

Settings

```
/etc/pandora/conf.d
```

After version 770 is installed for the first time, the `conf.d` directory is created, which will contain the files to add each additional process.

The `pandora_server/conf/pandora_server_sec.conf.template` file must be copied to the `conf.d` directory with a `.conf` extension with an appropriate name (for example `pandora_server_sec.conf`, `pandora_server_ter.conf` and so on).

The copied file must be edited to comply with the following operating rules:

- In the configuration file it must be defined with a unique server name (servername), it cannot be the same as the main process or another child process. Make sure it is not empty or commented.
- The secondary server must always be `master 0`, tasks on master will always be executed by the primary server.
- The configuration file must have the extension `.conf` and be inside the `conf.d` directory.
- The rest of the configurations will be defined in the same way as those of a standard pandora_server.
- Once a secondary server configuration file has been defined, the pandora_server service will manage both the main and secondary servers, starting, stopping or reporting the status of all processes that are configured.

```
[root@pandorafms pandora]# /etc/init.d/pandora_server status
Pandora FMS HA is not running.
pandorafms (/etc/pandora/pandora_server.conf) Server is running with PID: 25804.
greystone3 (/etc/pandora/conf.d/pandora_server_third.conf) Server is running with PID: 25859.
greystone1 (/etc/pandora/conf.d/pandora_server_sec.conf) Server is running with PID: 25930.
[root@pandorafms pandora]# echo $?
7
[root@pandorafms pandora]#
```

It must be taken into account that the pandora_ha process will only monitor the main process dynamically and that if it terminates, for any reason, the `pandora_ha` process will restart the entire stack (parent and child processes).

Web Console

The Pandora FMS Web Console requires a web server for its operation and uses various programming languages.

Apache web server

Apache Configuration

Pandora FMS has a series of folders with some files that complete its feature. To prevent these files from being accessed, some folders in the Web Console have an `.htaccess` file that restricts

their access. For this to be effective, in the Apache configuration you must allow these permissions to be overridden by `htaccess` . Therefore, set the `AllowOverride` token with the value `All`:

```
Allow Override All
```

instead of:

```
AllowOverrideNone
```

Configuration file config.php

Pandora FMS Web Console has a configuration file that is automatically generated during installation. Its location is: `/consolepath/include/config.php`.

For example, in CentOS systems it is located at:

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

The configuration options in the file are in the header of the file and are the following:

```
$config["dbtype"]
```

Type of database used. By default it is MySQL.

```
$config["dbname"]
```

Name of Pandora FMS database. By default it is `pandora`.

```
$config["dbuser"]
```

Username for the connection to Pandora FMS database. By default it is `pandora`.

```
$config["dbpass"]
```

Password for connection against Pandora FMS database.

```
$config["dbhost"]
```

IP address or name of the computer where Pandora FMS database is located. In reduced installations it is usually the same computer where the server is, this is `127.0.0.1` or `localhost`.

```
$config["homedir"]
```

Directory where Pandora FMS web console is installed. 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"]
```

This variable holds the value of the internal server URL for when using a reverse proxy such as Apache's `mod_proxy`.

Version 770 or later.

```
$config["id_console"]=id;
$config["console_description"]="description";
```

Where `id` is an integer greater than zero.

These two variables allow you to declare and add consoles to balance the load in the execution of Discovery server tasks.

- See also Discovery Console Tasks.
- See also Manage Consoles.
- See also Consoles dedicated to reports.

Apache Server Redirect

If you only have a Pandora FMS Web Console installed on your Apache server, you may want to automatically redirect to `/pandora_console` when users connect with the URL `/` of the web server. To do this you can create the following file `index.html` and place it in the root directory of the web server (`/var/www` or `/srv/www/htdocs`):

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

Configuration file php.conf

Version 768 or later: You may authenticate with API Token by sending in the HTTP headers of a bearer token generated by each user and for their

own private and particular use. See also “Edit my user”.

For header authentication with bearer token to work properly, the directive `HTTP_AUTHORIZATION=$1` must be included in the file `/etc/httpd/conf.d/php.conf` :

```
# Redirect to local php-fpm if mod_php (5 or 7) is not available
<IfModule !mod_php5.c>
   <IfModule !mod_php7.c>
     <IfModule !mod_php.c>
       # Enable http authorization headers
       SetEnvIfNoCase ^Authorization$ "(.+)" HTTP_AUTHORIZATION=$1
       <Proxy "unix:/run/php-fpm/www.sock|fcgi:localhost">
         ProxySet timeout=1200
       </Proxy>

       <FilesMatch \.(php|phar)$>
         SetHandler "proxy:fcgi:localhost"
       </FilesMatch>

     </IfModule>
   </IfModulee>
</IfModule>
```

Back to Pandora FMS documentation index