Monitoring with SNMP traps

Monitoring with SNMP traps

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

Introduction

Network devices that support SNMP, such as switches, routers, servers, printers, or Access Panels, can send alarms (SNMP traps) when certain events occur, such as an interface going down, or when CPU load or network power is very high, or if an uninterruptible power supply (UPS) changes state or a disk partition becomes full. Each device has its own collection of possible events, which is reflected in a collection, called a MIB, in this case, different from the MIB used to query the device.

Traps are sent only when something happens, asynchronously (not repetitively in time) by the device to an SNMP trap receiver. Pandora FMS has a trap reception console that allows you to view the traps sent by the monitored objects and add alerts to said traps. SNMP traps are received through the operating system daemon that the Pandora FMS SNMP server starts when the Pandora FMS server starts. SNMP traps are stored by default in:

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

The Pandora FMS SNMP console allows you to create rules to rename numerical OIDs to alphanumeric OIDs or simple descriptive text strings, so that it is more intuitive to work with SNMP traps. Pandora FMS also allows you to load trap MIBs from any manufacturer to automatically define those rules.

In order to work with SNMP traps, first modify the following parameter in `/etc/pandora/pandora_server.conf` to enable the SNMP Console:

```
snmpconsole 1
```

So that the traps SNMP appear translated (whether the variable links or the Enterprise SNMP chain) the following parameters must be activated:

```
translate_variable_bindings 1
translate_enterprise_strings 1
```

The `/etc/snmp/snmptrapd.conf` file must also be configured with the necessary parameters, for example:

```
authCommunity log public
disableAuthorization yes
```

With this configuration, traps will be created for the public community and will not require authorization.

SNMPv3

SNMPv3 traps are rejected unless the user sending them is added to `/etc/snmp/snmptrapd.conf` using the directive ''createUser''. For example:

```
disableAuthorization yes
createUser -e 0x0102030405 SNMPv3user SHA mypassword AES
```

The engineID must be specified with the `-e` option.
Otherwise, only SNMPv3 INFORMs will be received.

Access to the trap reception console

Operation → Monitoring → SNMP → SNMP Console. Using the magnifying glass icon in the first column you can display all the SNMP trap information, other important columns:

- Status: Green square if the trap has been validated and red if it has not been validated.
- SNMP Agent: Agent that sent the trap.
- Enterprise string: OID or Object Identifier of the sent trap. A trap can only send one piece of data in this field.
- Time Stamp: Time that has passed since the trap was received.

Colors

Additionally, SNMP traps have a color (seen as a background color) indicative of their corresponding type:

- Blue: Maintenance type.
- Purple: Information type.
- Green: `normal` type.
- Yellow: `warning` type.
- Red: `critical` type.

Validate traps

In order to effectively manage the traps, it is possible to validate them so that the administrator can discriminate between the traps that have been seen and those that are yet to be seen. To

validate a trap, click on the circle on the left or mark them and press the Validate button.

Delete traps

It is possible to delete traps once they have been processed, either individually or by multiple selection and Delete action.

To avoid accumulation, there is a configuration option that automatically deletes elapsed SNMP traps (by default more than 10 days old).

SNMP Trap Alerts

Introduction

Pandora FMS also has an alert system for the SNMP traps it receives. They are based mainly on filtering rules, searching for matches in all possible fields according to rules that you configure to trigger the alert.

Add an alert

SNMP trap alerts have several fields that will be used to match SNMP traps received on the console. You can useThe fields you want can optionally be used to create more general or more specific rules depending on the need. It is accessed through the menu Management → Alerts → SNMP alerts → Create. Important parameters:

- Enterprise String: Main OID of the SNMP trap. The presence of the chain will be searched, and it may even be a piece of the OID; for example `1.21.34.2.3` in a longer OID. It can be used in the same way in the field, and will perform the search as if it were: `*1.21.34.2.3*` (it is unnecessary to use asterisks as wildcard characters). For exact matches, end the string with the `$` character.
- Custom Value/OID: Searches the Value fields of the SNMP trap, as well as the Custom OID and Custom Value fields, that is, in the rest of the fields of TRAP. Search by regular expression works here. For example, if you have an SNMP trap that sends the string `Testing TRAP 225` it is possible to search for any trap with the substring `Testing TRAP` using the regular expression `Testing.*TRAP.*`
- SNMP Agent (IP): IP address of the Agent that sends the SNMP trap. It also allows you to use a regular expression or a substring.
- Trap type: Filter by trap type. Most of the traps generated are usually of type Other; If you don't specify anything, it will look for any type of trap.
- Single value: Filters by the trap value. This only refers to the single value of the primary OID, not any secondary OID.
- Variable bindings/Data #1-20: These are regular expressions that try to match variables 1 to 20. If there is a success, the alert is triggered. The value of the variable is saved in the corresponding

_snmp_fx_ macro (_snmp_f1_, _snmp_f2_, ...). Although only one regular expression can be specified for twenty variables, the _snmp_fx_ macros are available for all of them (_snmp_f11_, _snmp_f12_, ...).
- Alert Action: Combo where the action that will execute the alert is determined. If an event is chosen, the normal alert generation event will not be generated.
- Priority: Combo where the alarm priority is established.

The priorities of the alerts are different and have nothing to do with the priority of SNMP traps, nor with that of Pandora FMS events.

Field macros in alerts

The following macros can be used in any of the field fields of the alerts:

- _data_: Integer trap.
- _agent_: Name of the Agent.
- _address_: IP address.
- _timestamp_: SNMP trap date.
- _snmp_oid_: OID of the SNMP trap.
- _snmp_value_: SNMP trap OID value.

Working in environments with many traps

Trap storm protection

To do this, the following configuration parameters are used in the pandora_server.conf file:

- snmp_storm_protection: Maximum number of traps processed in the protection interval.
- snmp_storm_timeout: Trap storm protection interval in seconds. During that interval only X traps from the same source (same IP address) can be processed.
- snmp_storm_silence_period: If it is greater than 0, each time the storm protection is triggered for a specific source, the current time plus the silence time will be added. Until this time passes, new SNMP traps will not be registered for the specific source.

Trap storm protection, combined with traps filtering, allows that if hundreds of thousands are received a day, a few thousand can be worked on, avoiding redundant or useless.

Trap filtering on the server

Some systems receive a high number of SNMP traps of which only a small percentage is of interest to monitor. From Monitoring → SNMP → SNMP Filters different filters can be defined. Press the Create button, add a description and as many filters as you need with the + button.

Customize SNMP Traps

Trap renaming and customization

Please note that all previous traps will not change their appearance, this will take effect with new traps that enter the system from this point on.

Editing an SNMP trap is the process of customizing the appearance of an SNMP trap in the Web Console. To edit a trap, use the menu Operation → Monitoring → SNMP → SNMP trap editor.

The Custom OID is a Perl-compatible regular expression that will be compared to the part of the SNMP trap string that contains the variable bindings. It is not usually necessary to translate a trap.

Custom OID is not intended to contain the entire bindings variable string, which may be longer than the maximum length it supports, but rather a regular expression that matches one or more variables.

Upload manufacturer MIBs

This option is used to upload MIB and expand the internal Pandora FMS translation database, so that when an SNMP trap arrives, it is automatically translated by its description. It is accessed through the menu Operation → Monitoring → SNMP → MIB uploader.

Associate a trap with the rest of Pandora FMS alerts

Menu Management → Setup → Setup → Enterprise → Forward SNMP traps to an agent (if it exists).

If this option is changed, the Pandora FMS server service must be restarted for it to take effect.

This option (general to the server) forwards the SNMP trap to a special Agent Module called SNMPTrap as a text string, if and only if, the source IP address of the SNMP trap is defined as an agent's IP. When this occurs, the SNMP trap arrives as a line of text to the Agent within that Module, which is a Module that is defined only when the first SNMP trap arrives.

Text alerts can be specified on this Module, these being completely standard, like those of any

module. This allows you to customize SNMP monitoring so that certain traps from certain sources can be treated as another module, and thus integrate it into the rest of the monitoring, including alert correlation.

Another solution is to set up an alert on the SNMP trap that activates an agent module. For example, SNMP trap consists of writing to a log file, and you have an agent that reads that file and executes when there is a 1 written. In this way, the module will jump when the desired SNMP trap is received and the correlation can be established based on the received trap.

External SNMP trap manager

The SNMP console is limited to receiving SNMP traps, as it only processes TRAP as an individual entity, but an SNMP trap can contain a lot of information.

Sometimes it happens that the only monitoring that can be done is based on SNMP traps.

To do this, you can choose to process the information collected in an SNMP trap again through an external script, which acts as a plugin.

To do this, you must create a alert command that executes said script to post-process the received SNMP trap.

The application of this technology is extremely broad, which is why each script must be customized since it can have a very dynamic structure. In many systems, the information received is not only text, but also numerical, which can feed numerical information modules and thus represent graphs, etc. It will always be necessary to keep in mind that the data generated in the XML should always be of asynchronous type.

SNMP trap forwarding

With Pandora FMS it is possible to enable forwarding of SNMP traps to an external host by enabling the snmp_forward_trap in the token in the Pandora configuration file.

Independent management of the snmptrapd daemon

It is possible that for some reason you prefer to manage the snmptrapd daemon independently of

Pandora FMS (to stop or start it independently of the main Pandora FMS daemon). To do this, you must take several things into account:

1. You must also activate the `snmpconsole` parameter on the Pandora FMS server.

2. The logs configured on the Pandora FMS server must be the same as those generated in the independent call to snmptrapd

3. The call to snmptrapd must have a specific format since the call to the standard system daemon is invalid. The call should be like this (the `-A` parameter is especially important):

```
/usr/sbin/snmptrapd -A -t -On -n -a -Lf /var/log/pandora/pandora_snmptrap.log -p
/var/run/pandora_snmptrapd.pid --format1=SNMPv1[**]%4y-%02.2m-
%l[**]%02.2h:%02.2j:%02.2k[**]%a[**]%N[**]%w[**]%W[**]%q[**]%v\n --
format2=SNMPv2[**]%4y-%02.2m-%l[**]%02.2h:%02.2j:%02.2k[**]%b[**]%v\n
```

4. You must configure the token in the server configuration file:

```
snmp_trapd manual
```

5. When you establish this operation, you must perform the following operation:

- Change the configuration in `/etc/pandora/pandora_server.conf`.
- Stop the Pandora FMS server.
- End the snmptrapd process.
- Start upsnmptrapd manually (with the format indicated above).
- Start the Pandora FMS server.

Trap log file management

The snmptrapd process can be stopped and started without the need to stop and start the Pandora FMS server process, as long as the files `pandora_snmptrap.log.index` and `pandora_snmptrap.log` are not modified. If these files are modified, it is necessary to restart the Pandora FMS server. If you need to externally rotate the trap log, you must restart the Pandora FMS server after deleting the aforementioned files.

SNMP trap buffering

It is more efficient for the SNMP console to directly process traps from the snmptrapd log file. This configuration is recommended only if reliability or direct connectivity is a concern.

If SNMP traps are sent to an external manager over an unreliable connection, some information will be lost. Pandora FMS allows you to instead forward traps from a local snmptrapd to your Pandora FMS server in a reliable way.

Prerequisites:

- A local snmptrapd that is receiving traps.
- A local Pandora FMS agent.
- An installation of Pandora FMS.

snmp_extlog can be any file that the Pandora FMS server can write to, but it must be different from snmp_logfile (also defined in `/etc/pandora/pandora_agent.conf`).

Trap Generator

This tool allows you to generate custom SNMP traps that you can later view in the SNMP console. It is accessed through the menu Operation → SNMP → SNMP trap generator.

In SNMP Type choose an SNMP type from the following options:

- Cold Start: Indicates that the agent has been started or restarted.
- Warm Start: Indicates that the agent configuration has been modified.
- Link down: Indicates that the communication interface is out of service (inactive).
- Link up: Indicates that a communication interface has been activated.
- Authentication failure: Indicates that the agent received a request from an unauthorized (community controlled) NMS.
- EGP neighbor loss: Indicates that on systems where routers use the EGP protocol, a nearby host is out of service.
- Enterprise: This category contains all new SNMP traps, including those from vendors.

Return to Pandora FMS Documentation Index