Remote monitoring

Remote monitoring

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

Remote Monitoring

Introduction

The Network server executes the tasks assigned to it via a multithreaded queuing system, it can work with other network servers (HA mode).

You must have full visibility (IP addresses and ports) over which tests are going to be performed. This chapter also covers the Plugin server and WMI server.

Basic network monitoring

1. ICMP Tests: These are basic network tests that let you know if a host is online and accessible, as well as the time it takes to reach that device through the network.
2. TCP Tests: It is remotely verified that a system has the TCP port specified in the module definition open.
3. SNMP tests: It is possible to launch SNMP requests (SNMP Polling) to systems that have this service activated to obtain data such as the status of the interfaces, the consumption of network per interface, etc.

The Network server is the one who executes the different network tests assigned to each agent. Each agent is assigned to a network server, and it is this that is in charge of its execution, inserting the results in the Pandora FMS database.

Generic configuration of a module for network monitoring

To remotely monitor a computer or a computer service (FTP, SSH, etc.), the corresponding agent must first be created, accessed through the Management menu → Resources → Manage agents → Create agent. Fill in the details for your new agent and press the Create button.

Once you have created the agent, click on the upper tab of the modules (Modules). There select to create a new network module by pressing the Create button. In the next form that is displayed

select Create a new network server module, and when the dropdown menu on the right loads, select the desired check.

ICMP Monitoring

These are the most basic checks that provide important and accurate information.

- icmp_proc: Online check (ping) that lets you know if an IP address is responding or not.
- icmp_data: Latency check indicating the time in milliseconds to respond to a basic ICMP query.

TCP Monitoring

TCP is connection-oriented, so a TCP Send will correspond to a TCP Receive response that indicates the status of a port or a service to be monitored. Optionally, you can send a text string and wait to receive a response that will be directly treated by Pandora FMS as data.

- TCP Send: Field to configure the parameters to be sent to the TCP port. To send several strings in send/response sequence, you must separate them with the `|` character; supports the string `^M` to be replaced by sending a carriage return.
- TCP receive: Field to configure the text strings that must be compared with the responses received from the TCP connection. If sending/receiving in multiple steps, each step must be separated by the `|` character.

Example:

TCP Send

```
HELO myhostname.com^M|MAIL FROM: ^M| RCPT TO: ^M
```

TCP Receive

```
250|250|250
```

Remote execution modules

In order to successfully use these modules, the connection credentials of the agent to be monitored are required. Therefore, all this must be registered in the secure credential store. The instructions for the generic configuration of a module are repeated but one of the following is selected:

- `remote_execution_data`: numeric.
- `remote_execution proc`: boolean (0 FALSE, non-zero TRUE).
- `remote_execution_data_string`: alphanumeric (string).

- `remote_execution_data_inc`: incremental (ratio).

In addition, the following parameters must be defined:

1. Target IP: optionally the IP of the target (if not, the agent's will be used).
2. Port: optionally the port to connect to (22 in GNU/Linux, indifferent in MS Windows®).
3. Command: the command to execute to carry out the monitoring.
4. Credential identifier: the set of credentials to use to connect.
5. Connection method: optionally the connection method of the target (if not, the Agent's will be used).

The behavior of the module is identical when it comes to assigning alerts, generating events or viewing reports.

As of version 743, the `pandora_server.conf` file must have tokens for configuring the following parameters related to remote module execution: `ssh_launcher`, `rcmd_timeout` and `rcmd_timeout_bin`.

Common advanced properties of network modules

- Custom ID: allows you to store an ID of an external application to facilitate the integration of Pandora FMS with third-party applications. For example, a Configuration management database (CMDB).
- Interval: Module execution interval, which can be customized by an Administrator user in a predefined way and then used by standard users.
- Post process: for post-processing of the module (multiplying or dividing the returned value), for example when getting bytes and wanting to display the value in Megabytes.
- Min. Value and Max. Value: Any value below the minimum or above the maximum will be taken as invalid and discarded.
- Export target: Only available with Export server.
- Category: Only used in conjunction with the Command Center (Metaconsole).
- If Cron from is enabled, the module will be executed once when the current date and time match the date and time set in Cron from, ignoring the module's own interval.

SNMP Monitoring

Introduction to SNMP monitoring

- SNMP Polling: It is carried out from time to time actively and implies ordering Pandora FMS to execute a `get` command against an SNMP device.
- SNMP Trap: Occurs with changes or events on the device, which may or may not happen at any time. It is necessary to activate the SNMP trap console in Pandora FMS, where the ones received from any device will be displayed. Alerts can be defined through trap filtering rules for any of its fields.

Pandora FMS works with SNMP managing individual Object Identifiers or Object IDentifiers (OID), so each OID is a network module.

Necessary steps to work with SNMP

- Activate the SNMP management of the device so that SNMP queries can be made from the network server.
- Know the IP and SNMP community of the remote device.
- Know the specific OID of the remote device (or use one of the multiple wizards that Pandora FMS has or its SNMP OID explorer).
- Know how to manage the data returned by the device. SNMP devices return data in different formats. Pandora FMS can handle almost all of them. The counter type data are those that Pandora FMS manages “as remote_snmp_inc” and are of special importance, since being counters they cannot be treated as numerical data but as a rate of elements per second. Most of the SNMP statistical data is of the counter type and must be configured as `remote_snmp_inc` if it is to be monitored properly.

Monitoring with SNMP type network modules

Pandora FMS includes some OIDs in its database that you can use directly. MIBs are a collection of definitions that define the properties of the managed object within the device to be managed.

There are more MIBs included in Pandora FMS and with the Enterprise version MIB packages are included for different devices.

To be able to monitor any other element via SNMP, its SNMP community must be known. During module creation you must select Manual setup. In the Type field there are three options for SNMP, selecting one of them will expand the form showing the additional fields for SNMP.

- SNMP community: It is like a user ID or password that allows access to the statistics of a router or other device (SNMPv1 and SNMPv2c versions since SNMPv3 uses authentication by credentials). By default, devices come with a read-only public community (public) and generally each network administrator changes all community strings to custom values in the device configuration.
- SNMP OID: OID identifier to monitor, which consists of a string of numbers and periods. These strings are automatically translated into more descriptive alphanumeric strings if the corresponding MIBs are installed on the system.

Monitoring SNMP from Software Agents

A Software Agent is generally used to obtain local data, however it can also perform SNMP monitoring.

On GNU/Linux®

snmpget is usually installed by default, so it can be called from themodule_exec line.

```
module_exec snmpget -v <version> -c <community> <IP address> <numeric OID>
```

It should be noted that only “basic” OIDs are translatable by their numerical equivalent, and that it is advisable to always use numerical OIDs, since it is not known if the tool will know how to translate it or not. In any case you can always load the MIBs in the directory:

```
/usr/share/snmp/mibs.
```

On MS Windows®

snmpget.exe (which is part of the net-snmp project, licensed under the BSD license) is added to the Software Agent along with the basic MIBs, plus a wrapper to encapsulate the call. Similar to Linux, you can load the MIBs into the directory:

```
/util/mibs.
```

MIB Manager

Pandora FMS by default uses the MIBs that are hosted by the operating system in:

```
  /usr/share/snmp/mibs.
```

New MIBs can be added (and managed later) via the MIB uploader functionality from the Operation menu → Monitoring → SNMP.

These MIBs are only used by Pandora FMS and are stored in the route:

```
  {PANDORA_CONSOLE}/attachment/mibs.
```

This functionality only manages the MIBs for SNMP Polling,
in the case of SNMP Traps see the chapter Monitoring with SNMP traps.

Pandora FMS SNMP Browser

The SNMP Browser performs a complete walk-through of the device tree. This operation can take several minutes, and it is possible to traverse precise branches and shorten the traversal. It is accessed from Monitoring → SNMP → SNMP Browser.

The system will request that information from the system and will also display (if available) the requested OID information. If there is no information about the OID of the device, it is displayed only in numeric format. The descriptive information of the OIDs is stored by the managed information bases or MIB. If you don't have a MIB for the device you want to explore, you probably have to resort to looking for “pieces of information” in the information displayed by Pandora FMS,

which is complex and takes time.

The SNMP browser also allows you to search for a text string both in the obtained OID values and in the translated values of the OID themselves (if available). This is especially useful for searching for specific known strings and locating their OID. If it locates several entries, it will allow us to jump from one occurrence to another, and it will show them highlighted in yellow.

It is possible to select several OID and add them to an agent by clicking the Create agent modules button. To do this, the agents that will be monitored with said OID are selected and added to the box on the right. You can also select multiple OID to add to a monitoring policy.

Pandora FMS SNMP Wizard

SNMP Wizard

Administration view of an agent.

You must define the destination IP address, community and other optional parameters (SNMP v3 is supported) to do an SNMP Walk to the target. Once the information is received correctly, a form will appear for the creation of modules such as Devices, Processes, Free space on disk, Temperature sensors and Other SNMP data.

The type of module is selected and added to the creation list. When this process is finished, you can click on the Create Modules button.

This wizard will create two types of modules:

- SNMP modules for queries with static OID: Sensors, Memory, CPU, etc.
- Plugin modules for queries with dynamic OID or calculated data: Processes, Disk space, Used memory expressed as a percentage, etc.

For plugin type modules we will use the remote SNMP
plugin, so if the plugin is not installed on the system, these

features will remain disabled. The plugin should have the name snmp_remote.pl regardless of its location.

In order for the SNMP wizard to be able to obtain data from an SNMP device thanks to the remote components, it is necessary to meet 2 requirements:

- Have the Private Enterprise Number (PEN) of the device manufacturer registered in Pandora.
- Have the SNMP wizard components registered and enabled in Pandora for the device manufacturer.

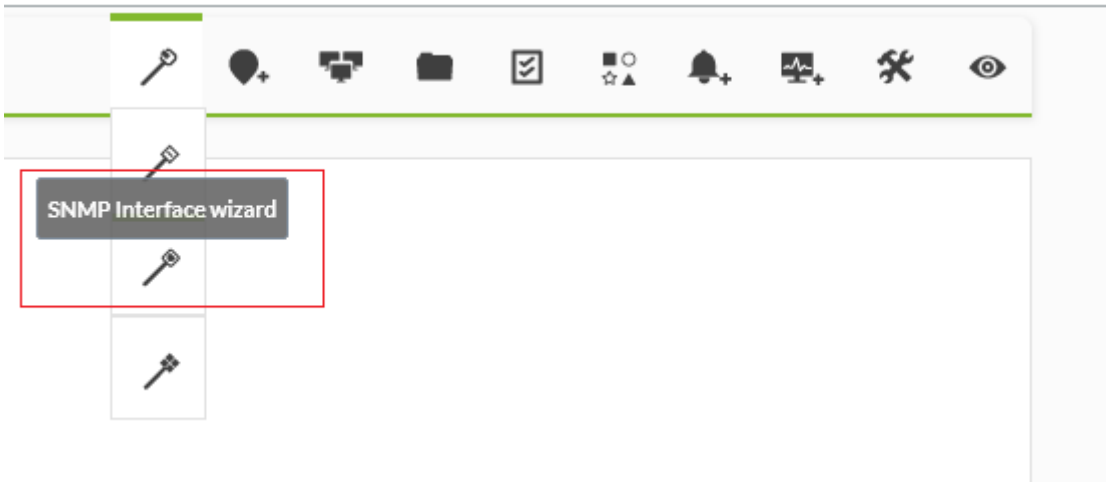
If the scanned device meets these requirements, all modules from which data could be obtained will be displayed to give the opportunity to select which to create and which not.

Once the Create modules button is pressed, a summary list of the chosen modules will be displayed.go with your setup. In this list you will see the modules that cannot be created, either because they already exist in the agent or because 2 or more modules with the same name have been configured in the wizard itself.

Take into account that if the value of the Module collected by the wizard is of type incremental or absolute incremental, said value is not the increment itself but a reference value. To obtain an incremental value, two readings are necessary, for this reason the value of the Module will indicate “zero” until the next reading is performed.

Before they are added to the agent, there will be one last chance to confirm the creation of these modules or to cancel it and continue modifying the output of the wizard.

SNMP interface wizard



This Wizard navigates the SNMP branch IF-MIB::interfaces, offering the possibility to create multiple modules of various interfaces with multiple selection. After selecting the destination IP address, community, etc., the system will make an SNMP query to the destination machine and fill in the module creation form.

In order for the interface SNMP wizard to obtain data from an SNMP device, the SNMP device must return data from the IF-MIB branch.

Once the creation of the modules has been confirmed, it will be re-evaluated one by one if they can be created or not, to avoid duplicate modules in the event that the same modules have been created by another means during the confirmation time.

We will be notified if the process could be completed successfully or, on the contrary, there has been a module that could not be created.

Remote monitoring of MS Windows with WMI

WMI is a technology used in the Microsoft® operating system (O.S.) to obtain remote information from computers running Windows®; It is available from the Windows XP version up to the latest versions. WMI allows you to obtain all kinds of information from the OS, applications and even hardware. WMI queries can be made locally with the Software Agent (by calling the OS API) or remotely.

In some systems, remote access to WMI is not activated and it must be activated to be able to be consulted from the outside.

It is necessary to enable the wmiserver component in the Pandora FMS server configuration file.

```
# wmiserver : 1 or 0. Set to 1 to activate WMI server with this setup
# DISABLED BY DEFAULT
  wmiserver 1
```

Queries are made in WQL, a kind of Microsoft®-specific SQL language, for any object that appears in the WMI system database.

To start monitoring by WMI, you must first create the corresponding agent, then click on the upper tab of the modules (Modules). Once there, select Create a new WMI server module and press the

Create. button

WMI specific fields:

- Namespace: WMI namespace; in some queries this field is different from empty string (default), depending on the information provider of the application being monitored.
- Key string: Optional, field to compare with the string returned by the query, and if the module exists, it returns 1 or 0, instead of the string itself.
- Field number: The number of the returned field starting from 0 (WMI queries can return more than one field). Most of the time it is 0 or 1.
- WMI Query: WMI query, similar to a SQL statement.

WMI Wizard

Used to navigate and create modules with WMI queries to a specific agent. In the Agent Wizard (tab in the administration view of an agent), click on the icon:

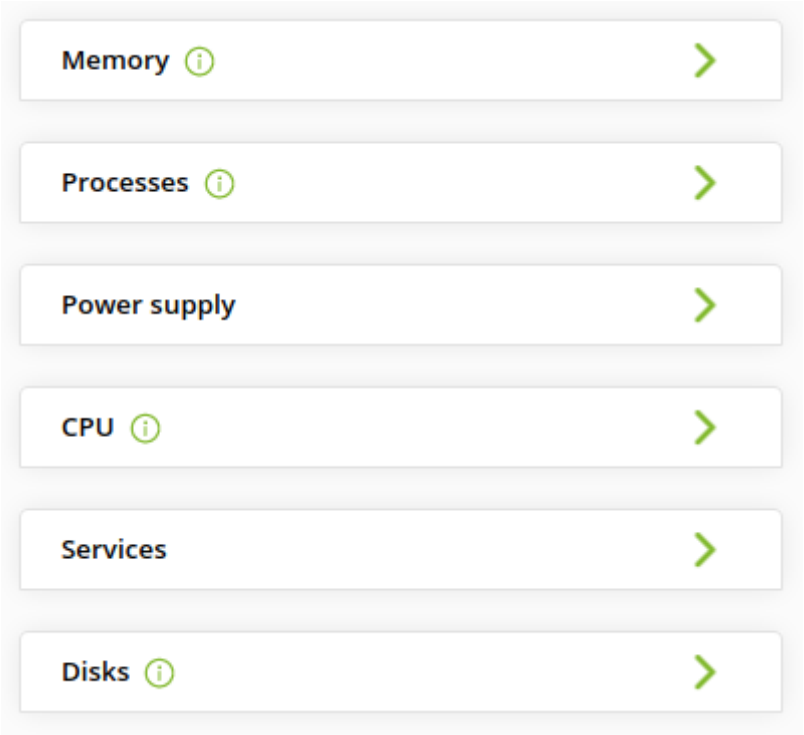
You must specify the username and password that have permissions to make WMI queries (or, failing that, the Administrator's) on the destination server to make the first WMI queries. This information will be used for the creation of modules.

With the WMI Wizard it is possible to create modules of different types of WMI information:

- Services: Boolean monitors will be created in normal state if the service is running and in critical state when it is stopped.
- Processes: Process monitors will receive information only when the process is active. Otherwise, they will fall into unknown state.
- Free disk space
- WMI Components: In this case it will choose between the WMI components registered in the system.

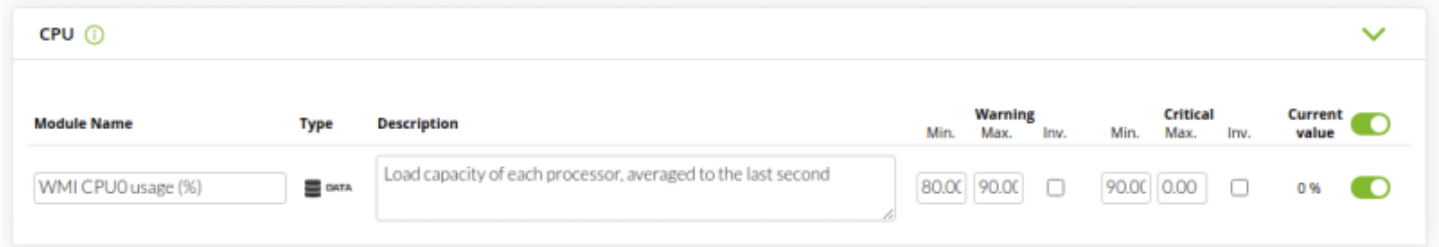
You must have WMI wizard components registered and enabled in Pandora: in this way, all the modules from which data could be obtained will be displayed in order to have the opportunityd to create them or not.

These modules will be shown organized in blocks based on the group to which the component of the wizard that generated them belongs.



All the blocks will be shown compressed at first to facilitate the visualization and they can be expanded to modify the selected ones or the data. In addition, in each block where modules have been marked for creation, you will see an informative icon that will indicate.

If we deploy a block, it will be possible to choose the modules that will be added and those that will not be added, as well as the option to modify the name, the description or the thresholds of each module individually.



Once the Create modules button is pressed, a list will be displayed with a summary of the chosen modules with their configuration. In this list you will see the modules that cannot be created, either because they already exist in the agent or because two or more modules with the same name have been configured in the same wizard.

Despite all the modifications that are made, there will be one last opportunity to confirm the creation of these modules or to cancel it and continue modifying the wizard result.

Once the creation of the modules has been confirmed, it will be re-evaluated one by one if they

can be created or not, to avoid duplicate modules in the event that the same modules have been created by another means during the confirmation time.

The wizard will notify you if the process could be completed successfully or if, on the contrary, there has been a module that could not be created.

Monitoring with remote server plugins

A remote plugin is a script or executable file that takes parameters and returns a single and unique value. The result could be a number, a boolean value (0 = error, OK <> 0), or a text string. A remote plugin usually allows input parameters. By default several server plugins come installed and ready to use and the user can always add the ones he needs.

There are two kinds of remote plugin: standard and type Nagios. The difference is mainly that the Nagios type respond with an error level and also, optionally, with a descriptive string.

Remote plugin management

It is accessed by Management → Servers → Plugins, a new window will open with a list of registered plugins. Each item has its corresponding edit and delete buttons, except if it has modules in use which can be listed using the Lock button.

When editing a plugin:

- Plug-in type: Allows you to establish whether it is standard or Nagios type.
- Max. timeout: To set the waiting time for its execution, special attention must be paid to this value since it must cover enough time for the execution otherwise it will not obtain any value.
- The description field is important since it will be seen in the user interface of the plugin, choose a short and explanatory legend.

- When executing a plugin, there are three wait values: the server's, the plugin's, and the module's. The one of the server prevails over the others, and secondly, the one of the plugin. For example, with server timeout values of 10 seconds, that of the plugin at 20 and that of a module with this plugin at 30, the maximum time that will wait for the execution of that module will be 10 seconds.
- When editing a plugin and it is in use by at least one agent, you will not be able to add or delete macros.

Internal Macros

In a similar way to alerts, you can also use internal macros in plugin settings. The supported macros are the following:

- `_agent_` or `_agentalias_`: Alias of the agent to which the module belongs.

- _agentname_: Name of the agent to which the module belongs.
- _agentdescription_: Description of the agent to which the module belongs.
- _agentstatus_: Current status of the agent.
- _address_: Address of the agent to which the module belongs.
- _module_: Name of the module.
- _modulegroup_: Module group name.
- _moduledescription_: Description of the module.
- _modulestatus_: Module status.
- _moduletags_: Labels (tags) associated to the module.
- _id_agent_: Agent ID, useful to directly build the URL or redirect to the Pandora FMS Console.
- _id_module_: Module ID.
- _policy_: Name of the policy to which the module belongs if one is established.
- _interval_: Module execution interval.
- _target_ip_: IP address of the destination of the module.
- _target_port_: Module destination port.
- _plugin_parameters_: Module plugin parameters.* _email_tag_: emails associated with module tags.

Custom field macros for remote monitoring

Custom field macros allow you to use the agent custom fields as macros for certain module configuration options.

Custom field macros work with SNMP, WMI, plug-in, and inventory type modules. They can be used in stand-alone modules, network components, and in policy modules.

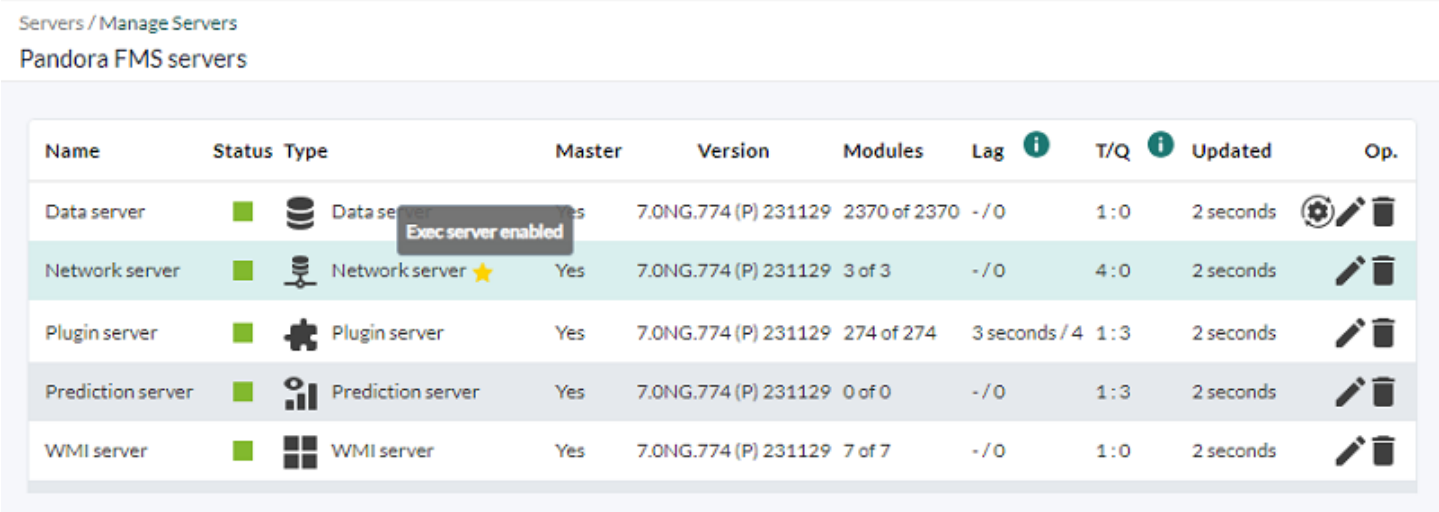
It is accessed by Management → Resources → Custom fields → Create field in this new custom field the SNMP community string will be stored. Note its ID, as it will later be part of the macro, and fill in the community string with the appropriate value in your SNMP agents.

Then you must create a componentes_de_red_componente_network SNMP to which you must enter _agentcustomfield_<n>_ as a string in SNMP community, where n is the ID of the custom field created.

Remote wizard and network test execution (Exec Server)

Only for PFMS servers installed on GNU/Linux.

This feature allows to execute some actions in remote Pandora FMS servers from Pandora FMS console.



Once you have configured at least one Exec server you may choose from:

- The SNMP browser in the SNMP section.
- The Event responses in the events section.
- The agent SNMP wizards.
- The agent WMI wizards.
- The agent SNMP interface wizards (except for Satellite Server).

Depending on the server selected when launching each *wizard*, the modules adapted for server or Satellite Server will be created. In the latter case, the modules will be written in the remote configuration file so that they can be executed by the server.

The Exec servers work internally through the execution of remote SSH commands from Pandora FMS console to the enabled servers, called Exec Server. These can be Network servers or Pandora FMS Satellite servers.

The configuration process will require the assistance of the person in charge of network administration to configure both PFMS servers and the target computers and the connection and data traffic, among other aspects such as firewalls and VLAN to increase security.

- You must have a logical agent configured with remote configuration enabled.

Without remote configuration enabled you will lack the ability to create Satellite modules from the wizards (*wizards*).

- You must have created digital keys (public key and private key) for the SSH connection.
- The public key must be copied to the target servers and must be configured to only connect that way, by digital key.
- On the server running the PFMS Web Console, you must have a user created at operating system level and with proper access to its own directory and which allows to execute a valid *shell* for the tasks to be entrusted.
- In PFMS Web Console you must log in as user *superadmin* or *Pandora Administrator*.

See the technical annex for more information.

Route monitoring

Pandora FMS offers by default the monitoring of complete routes between two points in the network, visually indicating the path that is being followed at all times to communicate between these two points. Pandora FMS route analyzer uses an agent plugin to map the route.

To use this system you need:

- A software Agent at the point of origin of the route to be analyzed.
- Reach via ICMP from the point of origin.

Optionally, if you want to do route scans over the Internet, it is recommended that you deploy the MTR application on the route source computer.

Access the agent plugins configuration tab and add the following line:

```
route_parser -t <target_address>
```

Finally activate the execution of the plugin.

Back to Pandora FMS documentation index