



Удаленный мониторинг



from:

<https://pandorafms.com/manual/!776/>

Permanent link:

https://pandorafms.com/manual/!776/ru/documentation/03_monitoring/03_remote_monitoring

2024/06/10 14:34



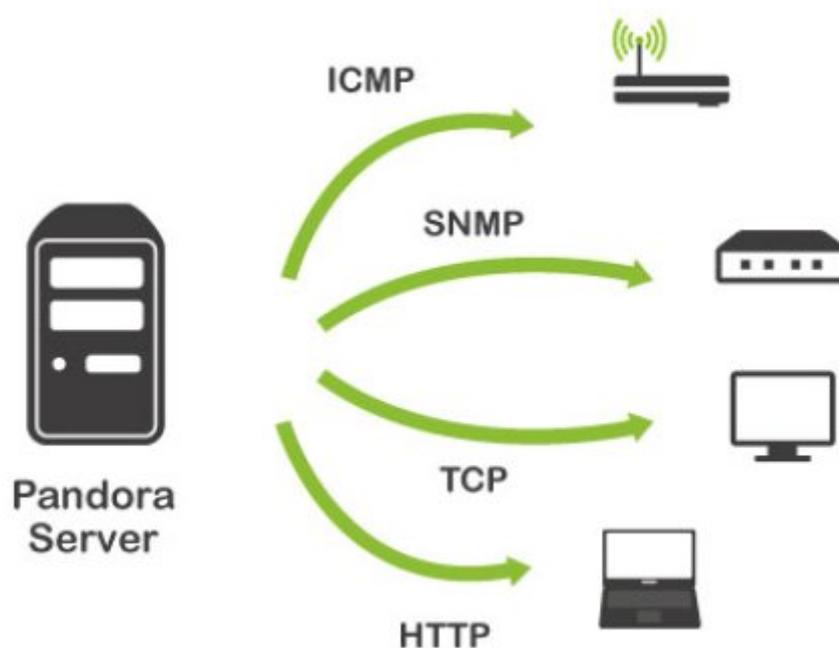
Удаленный мониторинг

[Вернуться в оглавление Pandora FMS](#)

Удаленный мониторинг

Введение

Сетевой сервер (*Network Server*) Pandora FMS является ключевым элементом, поскольку он позволяет выполнять тесты удаленно и централизованно. В отличие от [Сервера Данных](#), Сетевой Сервер выполняет поставленные перед ним задачи с помощью многопроцессной системы очередей. Кроме того, Сетевой Сервер может работать с другими [Сетевыми Серверами \(режим HA\)](#), балансируя нагрузку и выступая в качестве резервной копии в случае выхода из строя другого Сетевого Сервера, принимая на себя работу, которую выполнял отключенный сервер.



Сетевой Сервер работает только с теми сетевыми модулями, которые ему назначены. Сетевой Сервер должен иметь полную видимость (IP-адреса и порты) тех элементов, которые будут подвергаться тестированию. Однако межсетевые экраны (*firewalls*) как физически (в *firmware маршрутизаторов*), так и программно (на уровне операционной системы) могут препятствовать выполнению этой задачи, поэтому следует обратить пристальное внимание на создание соответствующих политик безопасности для

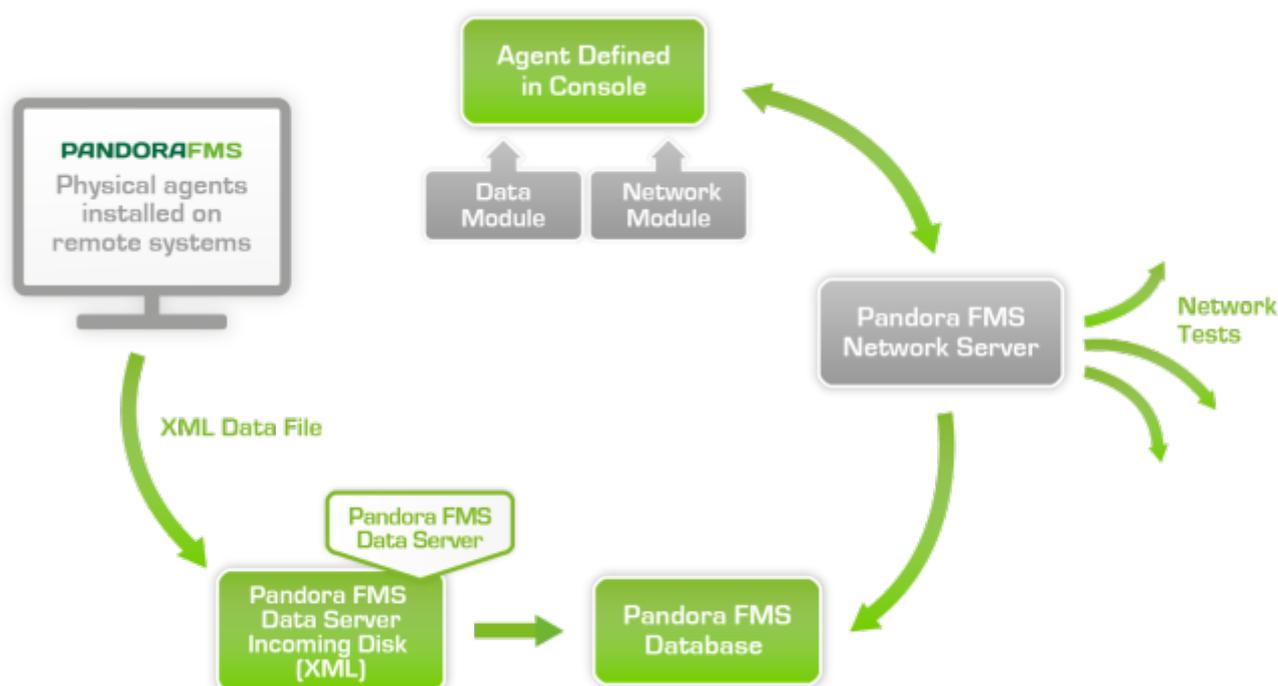
выполнения работы по мониторингу.

В дополнение к Сетевому Серверу существует множество других **подтипов серверов Pandora FMS**, которые могут выполнять удаленные тесты. В этой главе мы рассмотрим сетевые серверы, серверы удаленных плагинов и серверы, запускающие удаленные тесты на устройствах Windows. (*WMI Server*). Другие серверы, которые также выполняют удаленное тестирование, такие как тестовый WEB-сервер (*WEB Server* или *Goliath server*), имеют специальные главы документации.

Базовый мониторинг сети

Базовые сетевые модули Pandora FMS выполняют задачи удаленного мониторинга. Задачи удаленного выполнения можно свести к трем блокам.

1. Тестирование ICMP: это базовые сетевые тесты, которые позволяют узнать, находится ли хост в сети и доступен ли он, а также время, которое требуется, чтобы связаться с этим устройством по сети.
2. Тестирование TCP: удаленно проверяет, что в системе открыт TCP-порт, указанный в определении модуля. Кроме того, вы можете отправить текстовую строку и получить конкретный ответ, чтобы проверить правильность связи. Это позволяет вам реализовать простые проверки протокола, например, чтобы проверить, *жив ли HTTP-сервер*, вы посылаете строку GET / HTTP/1.0, ожидая получить строку 200 OK.
3. Тестирование SNMP: можно запускать SNMP-запросы (*SNMP Polling*) к системам, у которых включена эта служба, для получения таких данных, как состояние интерфейсов, потребление сети на интерфейс и так далее. Здесь описаны основные операции, а расширенные операции описаны в главе о **Мониторинге ловушек SNMP**



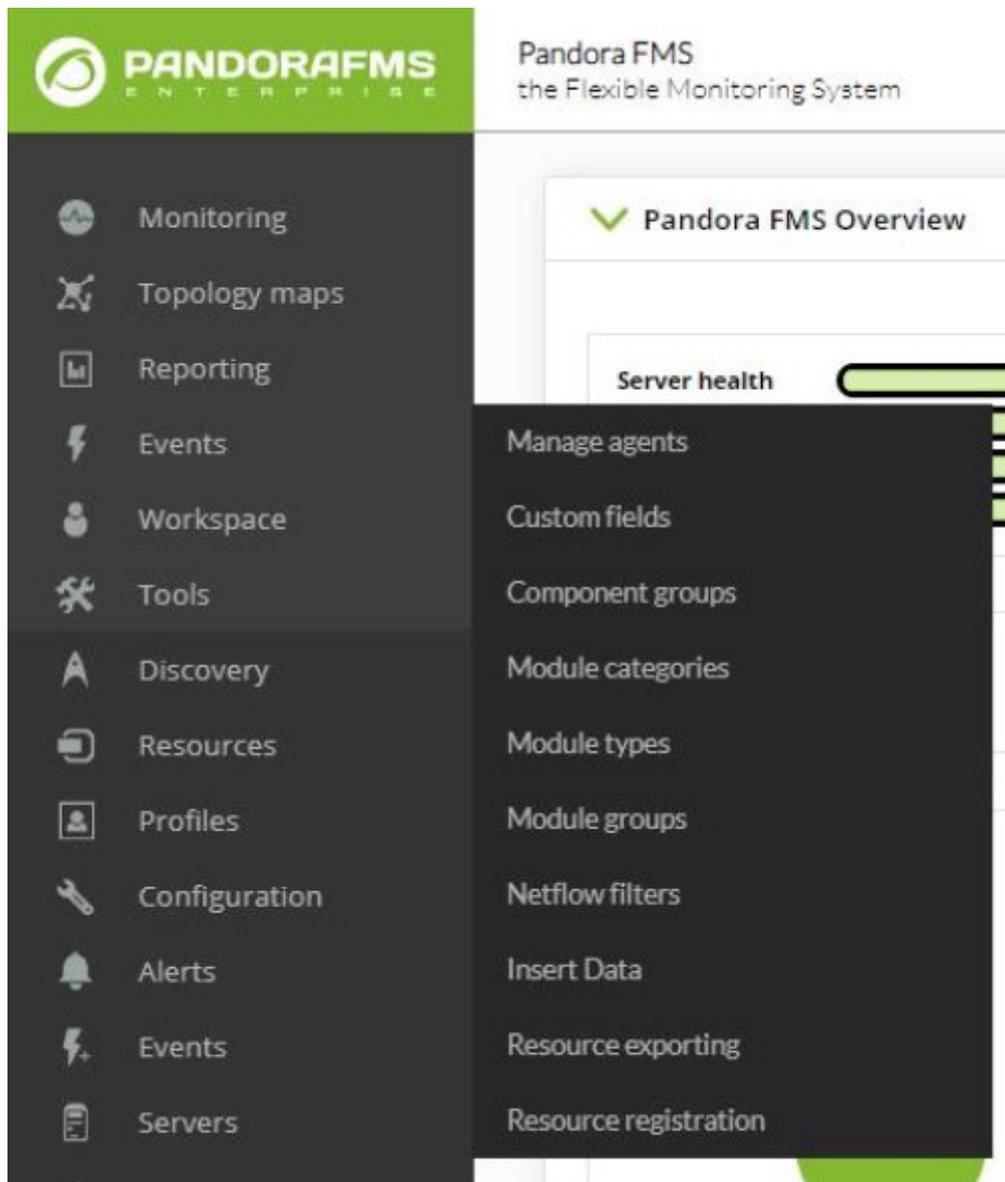
Именно сетевой сервер выполняет различные сетевые тесты, назначенные каждому агенту. Каждый агент закреплен за сетевым сервером, и именно он отвечает за его выполнение, вставляя результаты в базу данных Pandora FMS.

Общая конфигурация модуля для мониторинга сети

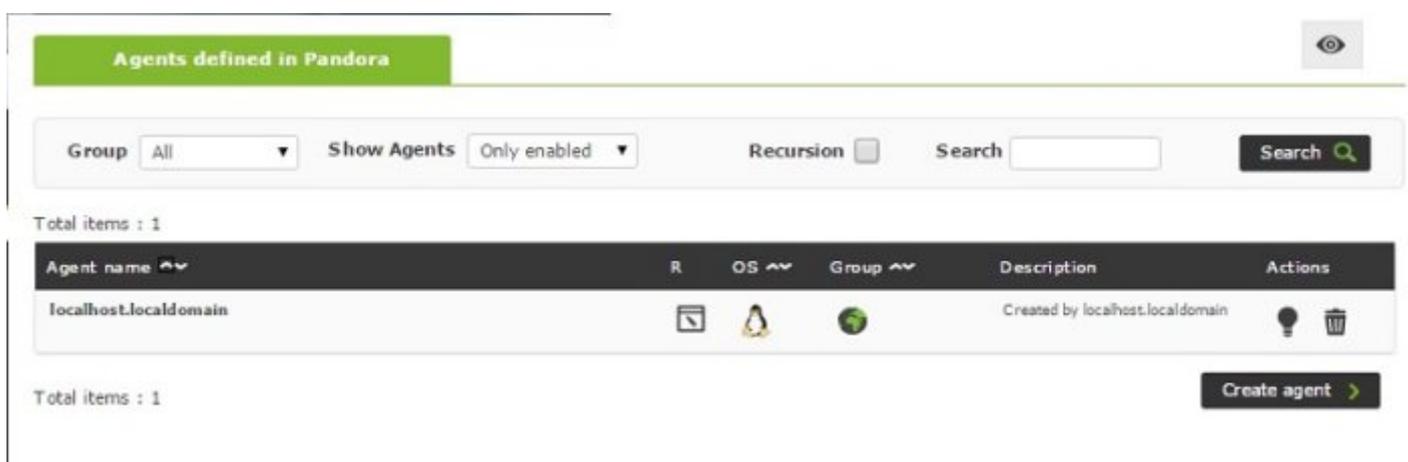
Для удаленного мониторинга устройства или службы устройства (FTP, SSH и т.д.) необходимо сначала создать соответствующий агент для мониторинга службы.

Когда мы говорим о создании агента, имеется в виду создание *Логического агента* в интерфейсе Pandora FMS, что отличается от установки **Программного Агента на целевом устройстве**.

Доступ к нему можно получить в разделе администрирования консоли Pandora FMS, Resources > Manage agents («Ресурсы» > «Управление Агентами»):



На следующем экране нажмите кнопку Create agent («Создать Агента»):



Заполните данные о новом агенте и нажмите кнопку. Create («Создать»):

Agent manager ?

Agent name ★

IP Address

Parent Cascade protection ?

Group Applications ▾

Interval 5 minutes ▾ ✎

OS Windows ▾ 🇺🇸

Server localhost.localdomain ▾ ?

QR Code Agent view

Only it is show when the agent is saved.

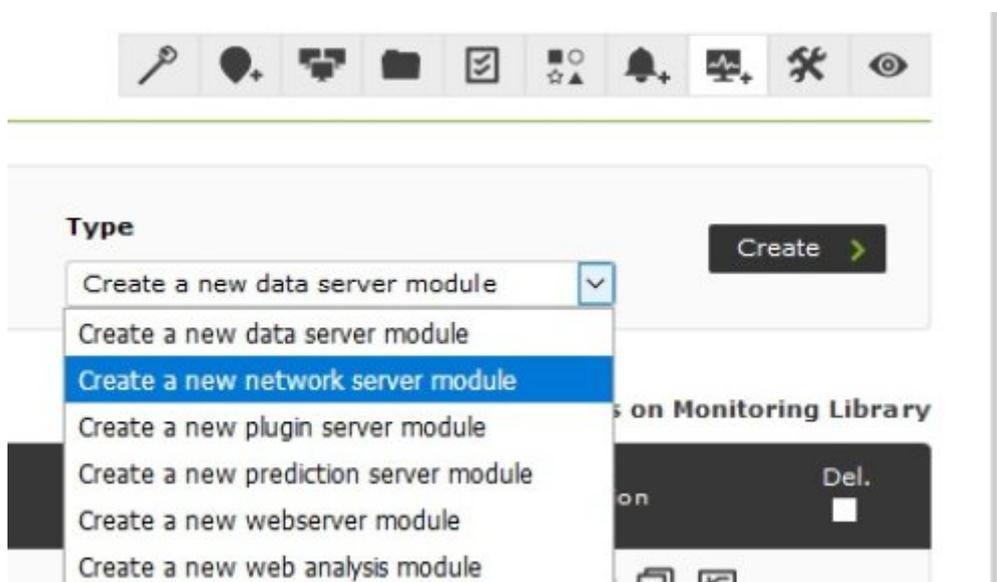
Description

⌵ Advanced options

⌵ Custom fields

Create ✎

После того как вы создали агента, нажмите на верхнюю вкладку модулей (Modules). Там выберите создать новый сетевой модуль и нажмите кнопку Create («создать»):



В форме ниже выберите модуль сетевого компонента, а когда загрузится выпадающее

меню справа, выберите нужную проверку.

Пример создания модуля Host Alive

Host Alive это простая проверка того, находится ли устройство в сети, путем выполнения *ping*.

The screenshot shows the configuration page for a 'Host Alive' module. At the top, there are dropdown menus for 'Using module component' (Network Management) and the module name (Host Alive). Below this, the 'Name' field is set to 'Host Alive', with a 'Disabled' checkbox and a 'Module group' dropdown set to 'Networking'. The 'Module parent' is 'Not assigned' and the 'Type' is 'Remote ICMP network agent'. The 'Dynamic Threshold Interval' is set to 'None'. Under 'Warning status', there are input fields for 'Min.' and 'Max.' (both set to 0) and an 'Inverse interval' checkbox. The same fields are present for 'Critical status'. The 'FF threshold' section has two radio buttons: 'Change all statuses' (selected) with a value of 0, and 'Change each status' with sub-fields for 'normal', 'warning', and 'critical' (all set to 0). The 'Historical data' checkbox is checked. The 'Target IP' field is empty, and the 'Port' is set to 0. On the right, a status bar shows 'Normal Status' (green), 'Warning Status' (yellow), and 'Critical Status' (red). Below the status bar is a large green square representing the current status.

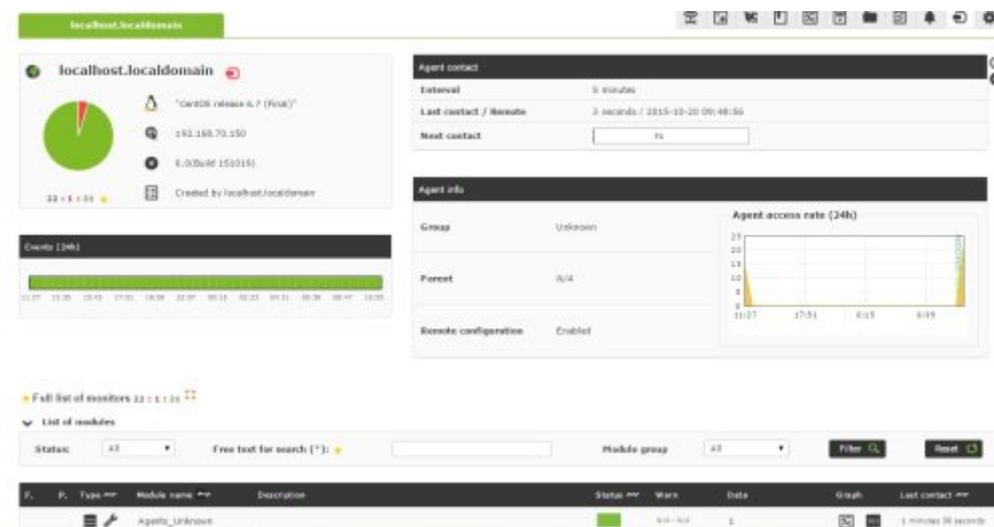
В поле *Target IP* необходимо указать целевой IP-адрес. После завершения определения модуля нажмите на кнопку Create («Создать»).

На следующем экране будут показаны модули для агента, стандартный *KeepAlive*, который создается вместе с агентом, и только что добавленный модуль *Host Alive*:



Предупреждение о модулях означает, что в модуль еще не поступили данные. Как только вы начнете получать данные, предупреждение исчезнет.

Чтобы просмотреть данные только что созданного модуля, нажмите на верхнюю вкладку View («Вид»), и в нем перейдите в самый низ, где будут отображаться данные после начала их приема:



Чтобы добавить другие типы сетевых проверок, действуйте аналогично описанному выше, но выбирая другие типы модулей.

Мониторинг ICMP

Приведенный выше пример является мониторингом ICMP. Это самые основные и простые проверки, которые дают нам важную и точную информацию.

- icmp_proc: проверка онлайн (ping) которая позволяет узнать, отвечает ли IP- адрес или нет.
- icmp_data: Проверка задержки, которая указывает время в миллисекундах для ответа на базовый запрос ICMP.

Мониторинг TCP

TCP ориентирован на соединение, поэтому за посланием TCP Send будет следовать ответ TCP Receive, указывающий на состояние порта или службы, за которой нужно следить. По желанию вы можете отправить текстовую строку и дождаться ответа, который будет обработан непосредственно Pandora FMS как данные.

TCP Send

Поле для настройки параметров для отправки на TCP-порт. Чтобы отправить несколько строк в последовательности отправки/ответа, разделите их символом |; поддерживается строка ^M, чтобы заменить ее отправкой возврата каретки. Пример:

```
GET / HTTP/1.0^M^M
```

TCP receive

Поле для настройки текстовых строк, которые будут сравниваться с ответами, полученными от TCP-соединения. Если они отправляются/получаются в несколько этапов, каждый этап должен быть отделен символом |.

Пример с Simple Mail Transfer Protocol (SMTP) на сервере электронной почты:

```
R: 220 mail.supersmtp.com ...
S: HELO myhostname.com
R: 250 myhostname.com
S: MAIL FROM:
R: 250 OK
S: RCPT TO:
R: 250 OK
S: DATA
R: 354 Start mail input; end with .
S: .....<your mail here>.....
S: .
R: 250 OK
S: QUIT
R: 221 mail.supersmtp.com Service closing ...
```

Текстовая строка 250 OK является ключевой во всех трех ответах для проверки правильности работы, поэтому подходящей настройкой является:

TCP Send

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

TCP receive

```
250|250|250
```

Если на первых трех этапах получен результат 250 OK, значит SMTP-сервер в порядке. Все это можно использовать для любого другого протокола, в котором используются сообщения с открытым текстом.

Модули удаленного выполнения

E Enterprise версия 741 или выше

- Remote execution data
- Remote execution data proc

- Remote execution data string
- Remote execution data inc

Для успешного использования этих модулей необходимы учетные данные подключения агента, который будет подвержен мониторинга. Поэтому все это должно быть записано в **безопасное хранилище учетных данных**:

Register new key into keystore

Identifier	<input style="width: 80%;" type="text"/>
Group	<input style="width: 80%;" type="text" value="All"/>
Product	<input style="width: 80%;" type="text" value="Custom"/>
User	<input style="width: 80%;" type="text"/>
Password	<input style="width: 80%;" type="password"/>

Пример создания нового модуля сетевого сервера:

Type ?	<input style="width: 80%;" type="text" value="Remote execution, numeric data"/>
Dynamic Threshold Interval	<input style="width: 80%;" type="text"/>
Warning status	<input style="width: 80%;" type="text"/>
Critical status	<input style="width: 80%;" type="text"/>

Remote execution, numeric data
Remote ICMP network agent, boolean data
Remote ICMP network agent (latency)
Remote TCP network agent, numeric data
Remote TCP network agent, boolean data
Remote TCP network agent, alphanumeric data
Remote TCP network agent, incremental data
Remote SNMP network agent, numeric data
Remote SNMP network agent, incremental data
Remote SNMP network agent, alphanumeric data
Remote SNMP network agent, boolean data
Remote execution, numeric data
Remote execution, boolean data
Remote execution, alphanumeric data
Remote execution, incremental data

Для удаленных запусков поддерживаются следующие типы ответных данных:

- remote_execution_data: цифровой.
- remote_execution proc: логический (0 ЛОЖЬ, ненулевой ПРАВДА).
- remote_execution_data_string: буквенно-цифровой (строка).
- remote_execution_data_inc: incremental (ratio).

Должны быть определены следующие параметры:

1. Target IP: опционально IP-адрес цели (если нет, будет использоваться IP-адрес агента).
2. Port: опционально порт для подключения (22 на GNU/Linux, безразлично на MS Windows®).
3. Command: команда для выполнения мониторинга.
4. Credential identifier: набор учетных данных для подключения.
5. Connection method: опционально метод подключения цели (в противном случае будет использоваться метод агента).

Пример:

Historical data

Target IP Port

Command

Credential identifier Manage credentials

Connection method
Inherited
SSH
Windows remote

✓ Advanced options

Система выполнит команду в отношении удаленному устройству, получая количество файлов во временном рабочем каталоге.



Пример с буквенно-цифровым типом данных для просмотра буквального вывода команды

Name ID 31 **Disabled**

Module parent **Module group**

Type ? *Remote execution, alphanumeric data (remote_cmd_string)*

Dynamic Threshold Interval  

Warning status Str: **Inverse interval**

Critical status Str: **Inverse interval**

Keep counters

FF threshold Change all statuses :
 Change each status : To 'normal' To 'warning' To 'critical'

Historical data

Target IP **Port**

Command

Credential identifier **Target OS**

Параметр 'Target OS' может быть настроен на наследование операционной системы агента, на которого вы нацеливаетесь.

Результат:



Current data at 2019-10-11 13:53:35

Volume in drive C has no label.
Volume Serial Number is 146E-D966

Directory of C:\

```
09/16/2019  04:28 PM           11,108 caca
11/07/2007  05:00 PM          17,734 eula.1028.txt
11/07/2007  05:00 PM          17,734 eula.1031.txt
11/07/2007  05:00 PM          10,134 eula.1033.txt
11/07/2007  05:00 PM          17,734 eula.1036.txt
11/07/2007  05:00 PM          17,734 eula.1040.txt
11/07/2007  05:00 PM             118 eula.1041.txt
11/07/2007  05:00 PM          17,734 eula.1042.txt
11/07/2007  05:00 PM          17,734 eula.2052.txt
11/07/2007  05:00 PM          17,734 eula.3082.txt
11/07/2007  05:00 PM           1,110 globdata.ini
11/07/2007  05:03 PM        562,688 install.exe
11/07/2007  05:00 PM           843 install.ini
11/07/2007  05:03 PM         76,304 install.res.1028.dll
11/07/2007  05:03 PM         96,272 install.res.1031.dll
11/07/2007  05:03 PM         91,152 install.res.1033.dll
11/07/2007  05:03 PM         97,296 install.res.1036.dll
```

Поведение модуля идентично при назначении предупреждений, генерации событий или визуализации отчетов.

Начиная с версии 743 в файле `pandora_server.conf` необходимо иметь *токены* для настройки следующих параметров, связанных с удаленным выполнением модулей: `ssh_launcher`, `rcmd_timeout` и `rcmd_timeout_bin`.

Общие расширенные свойства сетевых модулей

Description	<input type="text"/>		
Custom ID	<input type="text"/>	Unit	<input type="text" value="none"/>
Interval	Now (Agent interval x 0)	Post process	<input type="text" value="0"/>
Min. Value	<input type="text"/>	Max. Value	<input type="text"/>
Export target	<input type="text" value="None"/>	Discard unknown events	<input type="checkbox"/>
FF interval	<input type="text" value="0"/>	FlipFlop timeout	Disabled

- Custom ID: позволяет хранить идентификатор внешнего приложения для облегчения интеграции Pandora FMS с приложениями сторонних производителей. Например, *Configuration management database*. (CMDB).
- Interval: интервал выполнения модуля, который **может быть настроен заранее** пользователем Администратором определенным образом, а затем использоваться стандартными пользователями.
- Post process: для постобработки модуля (умножение или деление возвращаемого значения), например, когда вы получаете байты и хотите отобразить значение в мегабайтах.
- Min. Value у Max. Value: любое значение ниже минимального или выше максимального будет считаться недействительным и отбрасываться;
- Export target: доступно только в версии Enterprise и при наличии настроенного **Сервера Экспорта**.

Cron

Если *Cron from* включен, модуль будет запускаться один раз, когда текущие дата и время совпадают с датой и временем, установленными в *Cron from*, игнорируя собственный интервал модуля.

Вы можете указать временные периоды, в которые выполняется модуль; они имеют номенклатуру: Минута, Час, День месяца, Месяц, День недели, и существует три различных варианта:

- Cron from устанавливается по умолчанию во всех полях Any (Любой), без ограничения времени для мониторинга.
- Если Cron from → некоторое конкретное значение и Cron to все в Any: будет выполняться только при совпадении с заданным числом. Пр: 15 20 * * *, будет запускаться каждый день только в 20:15.
- Cron from → некоторое определенное значение и Cron to → → некоторое определенное значение: будут выполняться в течение выставленного интервала. Пр: 5 * * * * и 10 * * * * *, выполняется каждый час между минутами 5 и 10 (это эквивалентно 5-10 * * * * *).

Например, запускать каждый понедельник в 6:30:

Hour	Minute	Day of the month	Month	Day of the week
6	30	Any	Any	Monday

Например, выполнять каждый день между 6 и 7 часами:

Hour	Minute	Day of the month	Month	Day of the week
6	Any	Any	Any	Any

Hour	Minute	Day of the month	Month	Day of the week
7	Any	Any	Any	Any

Для локальных модулей мы добавляем строку `module_crontab`, соответствующую файлу [конфигурации агента](#).

Timeout

Время, в течение которого агент ожидает выполнения модуля, выраженное в секундах.

Category

Эта категоризация не влияет на обычный пользовательский интерфейс. Она предназначена для использования в сочетании с [Метаконсоли](#).

Мониторинг SNMP

Введение в мониторинг SNMP

Простой протокол управления сетью или *Simple Network Management Protocol (SNMP)*, определенный в [RFC 3411](#) и [RFC 3418](#) и опубликован IETF, работает как с синхронными, так и с асинхронными операциями:

- Polling SNMP: выполняется каждый раз активным способом и подразумевает приказ Pandora FMS выполнить команду `get` в отношении SNMP-устройства. Они выполняются путем создания сетевых модулей в Pandora FMS обычным способом.
- Trap SNMP: происходит из-за изменений или событиями в устройстве, которые могут произойти в любое время или нет (например, вентилятор перестает работать и температура оборудования повышается). Необходимо активировать консоль `SNMP traps` в Pandora FMS, где будут показаны `traps` полученные от любого устройства. Оповещения могут быть определены с

помощью правил фильтрации *ловушек* по любому из их полей.

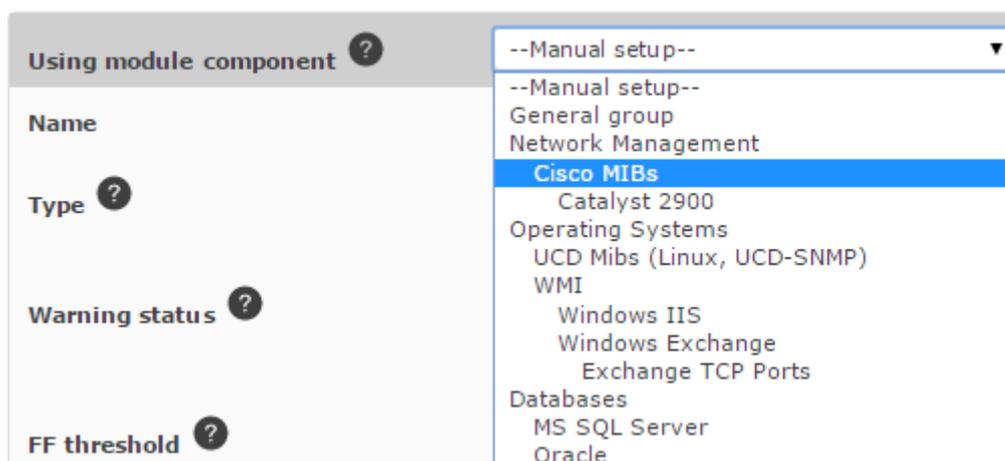
Pandora FMS работает с SNMP, управляя отдельными идентификаторами объектов или *Object Identifier* (OID), поэтому каждый OID представляет собой сетевой модуль. Пример: Чтобы узнать рабочее состояние каждого порта, а также входящий и исходящий трафик 24-портового Cisco Catalyst®, необходимо определить в общей сложности 72 модуля (24 x 3).

Этапы, необходимые для работы с SNMP

- Включить SNMP-управление устройством, чтобы можно было выполнять SNMP-запросы с сетевого сервера.
- Узнать IP-адрес и SNMP-сообщество удаленного устройства.
- Узнать конкретный OID удаленного устройства (или использовать один из многочисленных *wizards*, доступных в Pandora FMS или ее SNMP OID explorer).
- Узнать, как управлять данными, возвращаемыми устройством. SNMP-устройства возвращают данные в различных форматах. Pandora FMS может обработать почти все. Данные типа счетчика - это те данные, которыми управляет Pandora FMS as `remote_snmp_inc`, и они имеют особое значение, поскольку, будучи счетчиками, они не могут рассматриваться как числовые данные, а рассматриваются как количество элементов в секунду. Большинство статистических данных SNMP относятся к типу счетчиков и должны быть настроены как `remote_snmp_inc`, если вы хотите осуществлять мониторинг должным образом.

Мониторинг с помощью сетевых модулей типа SNMP

Pandora FMS включает в свою базу данных некоторые OID, которые вы можете использовать напрямую. Например, при создании модуля выберите компонент Cisco MIBs, чтобы отобразить список проверок с переведенными OID, доступных для Cisco:



Выбрав этот компонент, вы можете выбрать один из доступных для него OID, и поля будут заполнены необходимой информацией:



Нажмите на кнопку Create («Создать»). Для просмотра данных только что созданного модуля нажмите на верхнюю вкладку View («Вид»), а в ней перейдите в самый низ, где будет показан SNMP-график в реальном времени с помощью Graph (как только данные начнут поступать).

F	R	Type	Module name	Description	Status	Thresholds	Data	Graph	Last contact
			ping		■	N/A - N/A	1		3 minutes 49 seconds
			X0_ifHCInOctets	The total number of octets received on the interface, includ...	■	N/A - N/A	17,772.2		3 minutes 15 seconds
			X0_ifHCOutOctets	The total number of octets received on the interface, includ...	■	N/A - N/A	46,931		3 minutes 35 seconds
			X0_ifOperStatus	MAC C0:EA:E4:6E:9B:20	■	N/A - N/A	1		3 minutes 15 seconds
			X1_ifHCInOctets	The total number of octets received on the interface, includ...	■	N/A - N/A	486,441.6		3 minutes 35 seconds

В Pandora FMS включено больше MIB, а в версию Enterprise включены пакеты MIB для различных устройств.

Чтобы иметь возможность проводить мониторинг любого другого элемента по SNMP, мы должны знать его SNMP-сообщество. При создании модуля необходимо выбрать Manual setup:

Using module component ? **--Manual setup--**

Name Disabled Module group **General**

Module parent

Type ?

Dynamic Threshold Interval ?

Warning status ? Str.
Inverse interval

Critical status ? Str.
Inverse interval

FF threshold ? Change all statuses :
 Change each status : To 'normal' To 'warning' To 'critical'

Historical data

Target IP Port

SNMP community SNMP version

SNMP OID **SNMP walk** ?

User authentication Password authentication *

Privacy method Privacy pass *

Authentication method Security level

В поле Type есть три варианта для SNMP, при выборе одного из них форма развернется, показывая дополнительные поля для SNMP (для получения дополнительной информации можно воспользоваться видео-инструкцией.):

SNMP community **SNMP version**

SNMP OID **SNMP walk** ?

- **SNMP community:** это как идентификатор пользователя или пароль, который позволяет получить доступ к статистике маршрутизатора или другого устройства (версии SNMPv1 и SNMPv2c, поскольку SNMPv3 использует аутентификацию по учетным данным). По умолчанию устройства поставляются с публичным сообществом (public) только для чтения, и обычно каждый сетевой администратор изменяет все строки сообщества на пользовательские значения в конфигурации устройства.
- **SNMP OID:** Идентификатор OID для мониторинга, состоящий из строки цифр и точек. Эти строки автоматически переводятся в более описательные буквенно-цифровые строки, если в системе установлены соответствующие MIB.

MIBs - это набор определений, которые определяют свойства управляемого объекта в управляемом устройстве. По существу, это не совсем база данных, она только зависит от реализации. Каждый поставщик оборудования SNMP имеет под своим контролем уникальный раздел древовидной структуры MIB.

Пример буквенно-цифрового OID:

```
iso.org.dod.internet.private.transition.products.chassis.card.slotCps.cpsSlotSummary.cpsModuleTable.cpsModuleEntry.cpsModuleModel.3562.3
```

Его численный эквивалент:

```
1.3.6.1.4.868.2.4.1.2.1.1.1.3.3562.3
```

Мониторинг SNMP с помощью Программных Агентов

Удаленный мониторинг также может осуществляться с [Software Agent](#), который обычно используется для получения локальных данных, однако Pandora FMS обеспечивает гибкость в этом и во многих других аспектах.

В GNU/Linux®

snmpget обычно устанавливается по умолчанию, поэтому его можно вызвать из строки *module_exec*.

```
module_exec snmpget -v <versión> -c <comunidad> <dirección IP> <OID numérica>
```

Следует отметить, что только «базовые» OID могут быть переведены их числовым эквивалентом, и что рекомендуется всегда использовать числовые OID, поскольку неизвестно, будет ли инструмент знать, как перевести его или нет. В любом случае вы всегда можете загрузить mibs в каталог `/usr/share/snmp/mibs`.

Примеры:

```
module_begin
module_name SNMP_if3_in
module_type generic_data_inc
module_exec snmpget -v 1 -c public 192.168.55.1 .1.3.6.1.2.1.2.2.1.10.3
module_end
```

```
module_begin
module_name SNMP_Sysup
module_type generic_data
module_exec snmpget -v 1 -c public 192.168.55.1 DISMAN-EVENT-
MIB::sysUpTimeInstance
module_end
```

В MS Windows®

snmpget.exe (который является частью проекта net-snmp, с лицензией BSD) добавляется к Программному Агенту вместе с базовыми MIB, наряду с оберткой или скриптом (*wrapper* или *script*) для инкапсуляции вызова.

Синтаксис выполнения следующий:

```
module_exec getsnmp.bat <comunidad_SNMP> <ip de destino> <OID>
```

Аналогично Linux, вы можете загрузить MIBs в каталог /util/mibs.

Примеры:

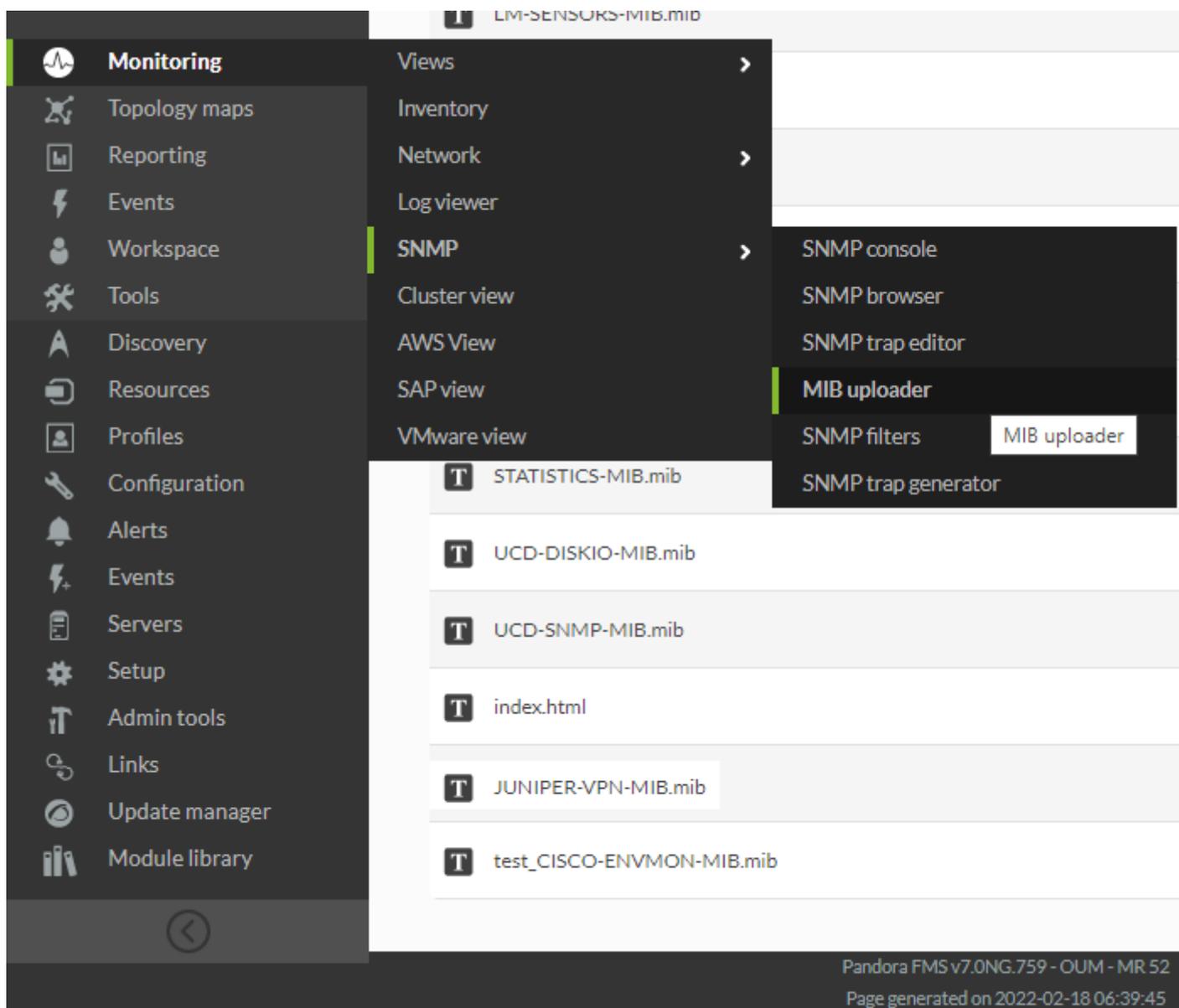
```
module_begin
module_name SNMP_if3_in
module_type generic_data_inc
module_exec getsnmp.bat public 192.168.55.1 .1.3.6.1.2.1.2.2.1.10.3
module_end
```

```
module_begin
module_name SNMP_if3_desc
module_type generic_data_string
module_exec getsnmp.bat public 192.168.55.1 IF-MIB::ifDescr.3
module_end
```

```
module_begin
module_name SNMP_Sysup
module_type generic_data
module_exec getsnmp.bat public 192.168.55.1 DISMAN-EVENT-MIB::sysUpTimeInstance
module_end
```

Менеджер MIBS

Pandora FMS по умолчанию использует MIBs, которые размещены в операционной системе по адресу /usr/share/snmp/mibs. Новые MIB могут быть добавлены (и затем управляться) с помощью функции MIB uploader. Эти MIB используются только в Pandora FMS и хранятся в {PANDORA_CONSOLE}/attachment/mibs.



Эта функциональность только управляет MIB для *Polling SNMP*, в случае *Trap SNMP* см. главу [Мониторинг с помощью SNMP-ловушек](#).

SNMP Браузер Pandora FMS

Версия Enterprise NG 744 или выше

SNMP Браузер выполняет полный обзор дерева устройства, и эта операция может занять несколько минут. Также можно проверить определенные ветви и сократить маршрут. Чтобы получить доступ, вы должны зайти на `Monitoring > SNMP > SNMP Browser`.

Например, чтобы получить информацию только о Cisco, вы можете просмотреть sub-MIB enterprise Cisco®, которое начинается с :

.1.3.6.1.4.1.9

Проводник используется для «поиска», то есть для разворачивания ветвей и получения значений. Система запросит эту информацию у системы, а также отобразит (если доступно) запрошенную информацию OID. Если для устройства нет информации OID, она отображается только в числовом формате. Описательная информация OIDs хранится посредством управляемых информационных баз или MIBs ([Management_Information_Base](#)). Если у вас нет MIB для устройства, которое вы хотите просканировать, вероятно, вам придется прибегнуть к поиску «кусочков информации» в информации, отображаемой Pandora FMS, что сложно и требует времени.

SNMP explorer также позволяет искать текстовую строку как в полученных значениях OID', так и в переведенных значениях самих OID' (если они доступны). Это особенно полезно для поиска определенных известных строк и определения их OID. Если он обнаружит несколько записей, он позволит нам переходить от одного события к другому, и покажет их выделенными желтым цветом.

SNMP BROWSER

Target IP: 192.168.50.1 Community: artica06 Starting OID: .1.3.6.1.2 Version: v. 1 Server to execute: Local console Browse

Search options

- SNMPv2-MIB
 - sysDescr
 - sysObjectID
 - sysContact
 - sysName
 - 0
 - sysLocation
 - sysServices
 - snmpInPkts
 - snmpOutPkts
 - snmpInBadVersions
 - snmpInBadCommunityNames

OID Information

OID	SNMPv2-MIB::sysName.0
Numeric OID	.1.3.6.1.2.1.1.5.0
Value	pacifico
Type	STRING
Description	An administratively-assigned name for this managed node. By convention, this is the node's fully-qualified domain name. If the name is unknown, the value is the zero-length string.
Syntax	OCTET STRING (0..255)
Display hint	"255a"
Max. access	read-write
Status	current

Create network component

Можно выбрать несколько OID и добавить их к агенту, нажав на кнопку Create agent modules. Для этого выберите агентов, которые будут подвергаться мониторингу с помощью этих OID, и добавьте их в поле справа. Эти модули будут созданы, как только мы нажимаем кнопку Add modules.

PANDORAFMS
Pandora FMS
the Flexible Monitoring System

Enter keywords to search

SNMP Browser

Target IP: demo.snmplabs.com Community: public Starting OID: system

Version: v. 2c Server to execute: Local console Browse

Search options

- SNMPv2-MIB
 - sysDescr
 - sysObjectID
 - 0
 - sysContact
 - sysName
 - 0
 - sysLocation
 - sysServices
 - sysORLastChange
 - sysORID
 - sysORDescr
 - sysORUpTime
- DISMAN-EVENT-MIB

Create agent modules Create policy modules Create network components

Add modules

Filter group: All

Search:

Agents available: pandorafms agent, pandorafms

Agents to apply: None

Cancel Add modules

Вы также можете выбрать несколько OID для добавления в политику, нажав на кнопку Create policy module.

Pandora FMS
the Flexible Monitoring System

Enter keywords to search

SNMP Browser

Target IP: demo.snmplabs.com Community: public Starting OID: system

Version: v.2c Server to execute: Local console Browse

Search options

SNMPv2-MIB

- sysDescr
- sysObjectID
 - 0
- sysContact
- sysName
 - 0
- sysLocation
- sysServices
- sysORLastChange
- sysORID
- sysORDescr
- sysORUpTime

DISMAN-EVENT-MIB

Create agent modules **Create policy modules** Create network components

Мы выбираем политики, в которые мы хотим добавить модульную конфигурацию этих OID. Чтобы создать новую политику для этих OID, нажмите на кнопку “Create new policy”.

Add modules

Filter group: All

Search:

Policies available:

- Basic Windows Monitoring
- Basic Linux Monitoring
- Basic Solaris Local Monitoring
- Basic AIX Local Monitoring
- Basic HP-UX Local Monitoring
- Basic Remote Checks

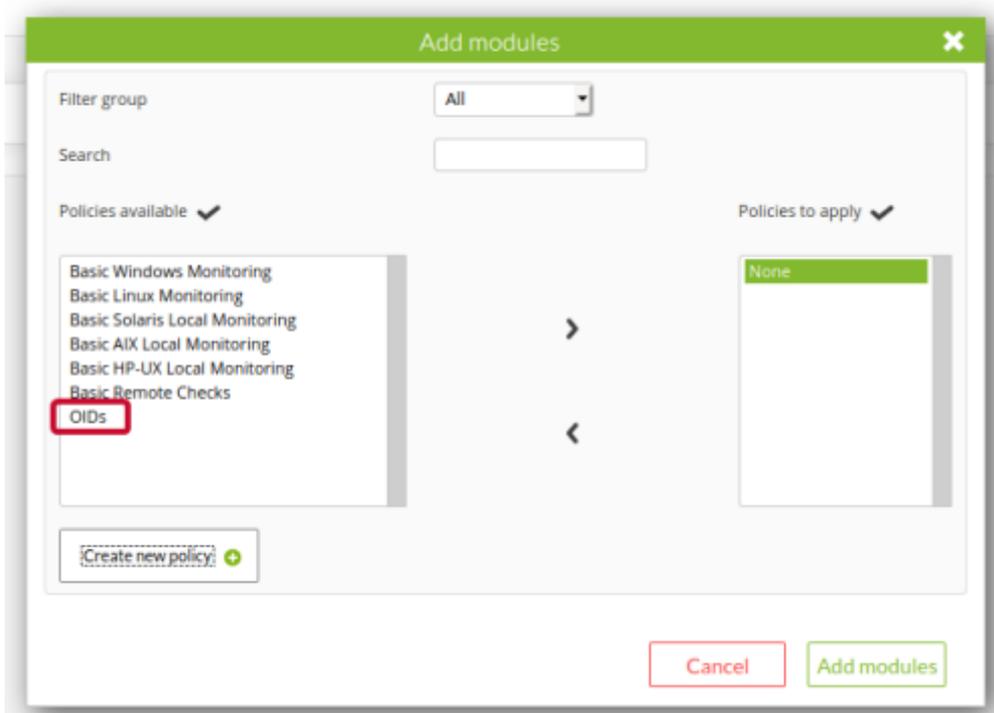
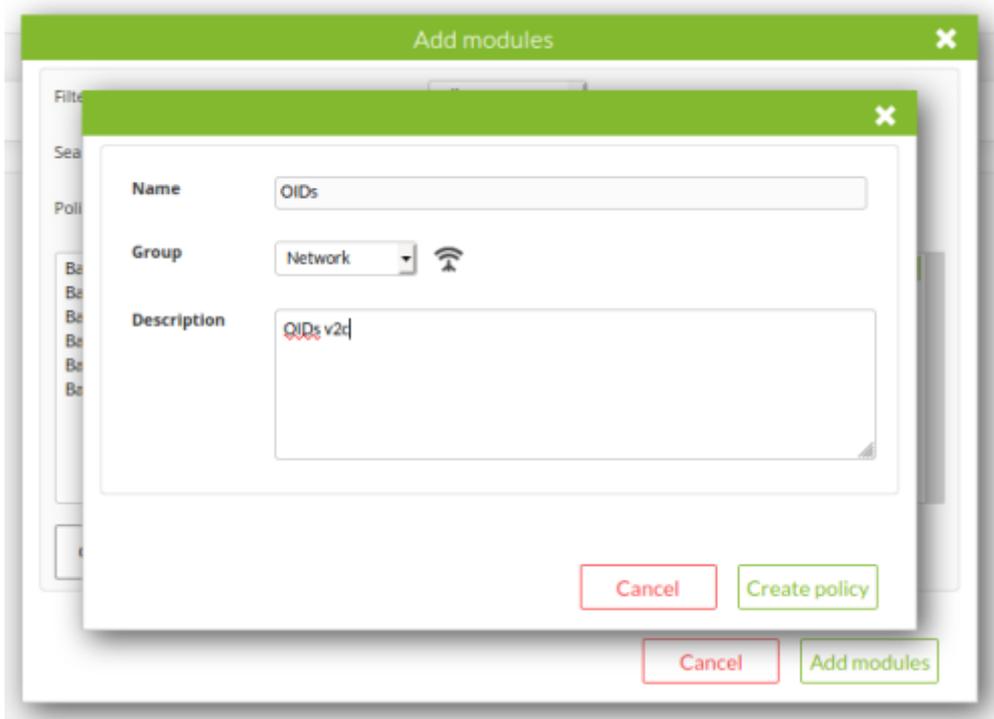
Policies to apply:

- None

Create new policy Cancel Add modules

Заполните поля, присвоив новой политике имя, группу и описание, и нажмите кнопку

“Create policy”. Затем добавьте их в поле справа и нажмите кнопку Add modules, чтобы эта конфигурация вступила в силу в политиках.



Для выбора конкретного OID можно воспользоваться кнопкой Create agent module. Эта кнопка позволяет выбрать конкретного агента и перенаправить на создание модуля внутри этого агента со всеми выбранными вами данными SNMP.

Pandora FMS
the Flexible Monitoring System

Enter keywords to search

SNMP Browser

Target IP: demo.snmplabs.com Community: public Starting OID: system

Version: v. 2c Server to execute: Local console Browse

Search options

SNMPv2-MIB

- sysDescr
- sysObjectID
- sysContact
- sysName
- sysLocation
- sysServices
- sysORLastChange
- sysORID
- sysORDescr
- sysORUpTime

DISMAN-EVENT-MIB

OID Information

OID: SNMPv2-MIB::sysObjectID.0

Numeric OID: .1.3.6.1.2.1.1.2.0

Value: .1.3.6.1.4.1.8072.3.2.10

Type: OID

Description: The vendor's authoritative identification of the network management subsystem contained in the entity. This value is allocated within the SMI enterprises subtree (1.3.6.1.4.1) and provides an easy and unambiguous means for determining "what kind of box" is being managed. For example, if vendor "Flintstones, Inc." was assigned the subtree 1.3.6.1.4.1.424242, it could assign the identifier 1.3.6.1.4.1.424242.1.1 to its "Fred Router".

Syntax: OBJECT IDENTIFIER

Max. access: read-only

Status: current

Create network component Create agent module

В редакторе модулей SNMP, когда вы редактируете или создаете сетевой модуль, вы можете запустить браузер SNMP, нажав кнопку «SNMP браузер», которая откроет его во всплывающем окне.

После того, как вы выбрали OID, который вы ищете, нажав на значок фильтра, этот OID будет выбран, и он автоматически перейдет в соответствующее поле определения модуля для его использования в нашем агенте.

Using module component: --Manual setup--

Name: [] Disabled [] Module group: General []

Module parent: Not assigned []

Type: []

Dynamic Threshold Interval: []

Warning status: []

Critical status: []

FF threshold: []

Historical data: []

Target IP: 192.168.50.1

SNMP community: artica06

SNMP version: v. 1 []

SNMP OID: []

Port: []

SNMP walk []

Search options:

- SNMPv2-MIB
 - sysDescr
 - sysObjectID
 - sysContact
 - sysName
 - sysLocation
 - sysServices

Use this OID Information

OID	SNMPv2-MIB::sysServices.0
Numeric OID	.1.3.6.1.2.1.1.7.0
Value	79
Type	INTEGER

A value which indicates the set of services that this entity may potentially offer. The value is a sum. This sum initially takes the value zero. Then, for each layer, L, in the range 1 through 7, that this node performs transactions for, 2 raised to (L - 1) is added to the sum. For example, a node which performs only routing functions would have a

SNMP Помощник Pandora FMS

В просмотре администрирования агента есть набор инструментов для массового создания дополнительных модулей: wizard (помощник) Агента.

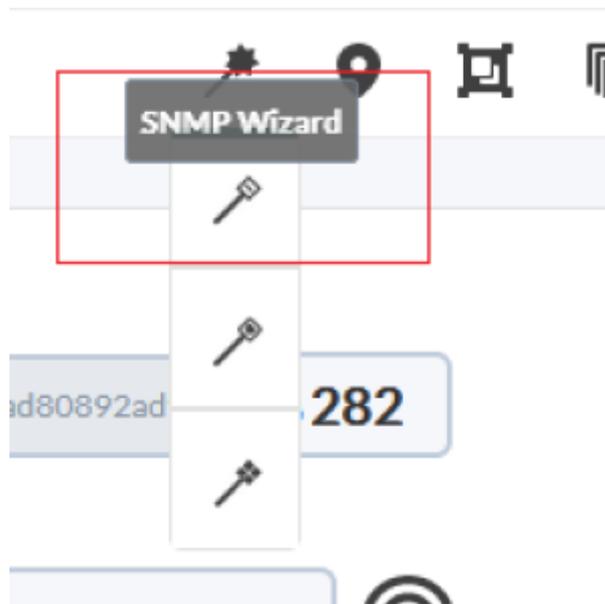
Agent wizard

Interval: 5 minutes

OS: Satellite

View agent QR code

Wizard SNMP



Вы должны определить IP-адрес назначения, сообщество и другие дополнительные параметры (поддерживается SNMP v3), чтобы выполнить *Walk* к устройству.

Target IP	192.168.80.1
Port	161
Server to execute command	Local console
SNMP community	
SNMP version	1

SNMP Walk >

Как только информация будет получена правильно, появится форма для создания модулей:

С помощью *Wizard* SNMP можно создавать модули различных типов данных SNMP:

- Devices: Устройства.
- Processes: Процессы.
- Free space on disk: Свободное место на диске.
- Temperature sensors: Температурные датчики.
- Other SNMP data: Другие данные SNMP.

Memory >

Other ⓘ >

Module Name	Type	Description	Warning				Critical				Current value	
			Min.	Max.	Inv.	%	Min.	Max.	Inv.	%		
Wizard network uptime	SNMP DATA	The time (in bundle	0.00	0.00	<input type="checkbox"/>	<input type="checkbox"/>	0.00	0.00	<input type="checkbox"/>	<input type="checkbox"/>	334 days 5 h... seconds	<input checked="" type="checkbox"/>

Sessions >

CPU >

Intrusions >

Antivirus >

Wizard ⓘ >

Module Name	Type	Description	Warning				Critical				Current value	
			Min.	Max.	Inv.	%	Min.	Max.	Inv.	%		
dmztest	SNMP TEXT		0.00	0.00	<input type="checkbox"/>	<input type="checkbox"/>	0.00	0.00	<input type="checkbox"/>	<input type="checkbox"/>	Empty	<input checked="" type="checkbox"/>
mgmttest	SNMP TEXT		0.00	0.00	<input type="checkbox"/>	<input type="checkbox"/>	0.00	0.00	<input type="checkbox"/>	<input type="checkbox"/>	Empty	<input type="checkbox"/>

Выберите тип модуля и переместите нужные элементы из комбинации слева в комбинацию справа. Когда этот процесс будет завершен, вы можете нажать на кнопку Create Modules (Создать Модули).

Этот *wizard* создаст два типа модулей:

- Модули SNMP для запросов со статическим OID: Датчики, Память, Процессор и т.д.
- Модули Plugin для запросов с динамическими OID или вычисляемыми данными: процессы, дисковое пространство, используемая память, выраженная в процентах, и т.д.

Для модулей типа плагин мы будем использовать удаленный плагин SNMP, поэтому если *plugin* не установлен в системе, эти функции останутся отключенными. Плагин должен иметь имя `snmp_remote.pl` независимо от расположения.

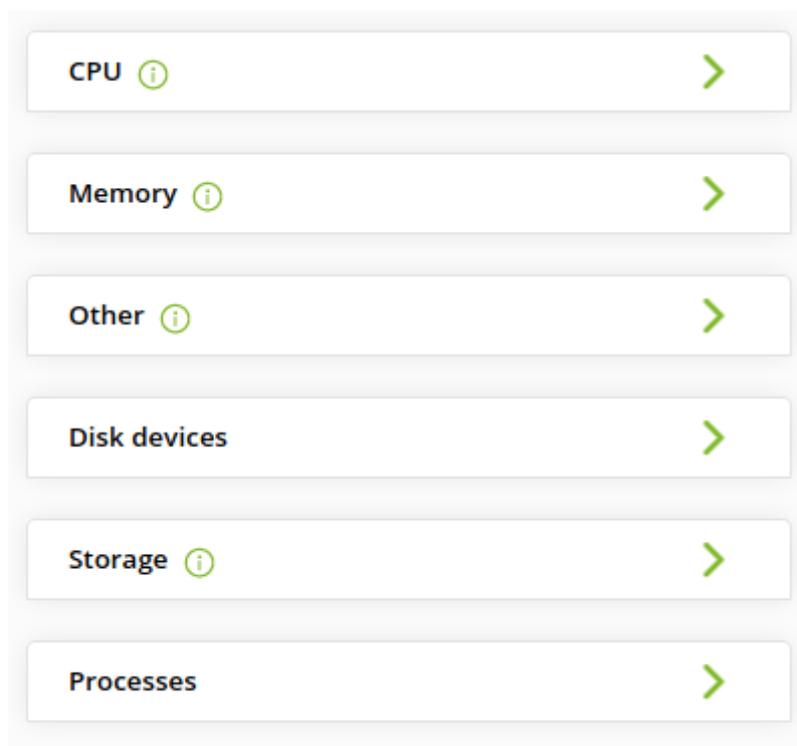
Для того чтобы *SNMP wizard* мог получать данные с SNMP-устройства благодаря удаленным компонентам, необходимо выполнить 2 требования:

- Быть зарегистрированным в Pandora с Private Enterprise Number (PEN) производителя устройства.
- Компоненты помощника SNMP в Pandora должны быть зарегистрированы и активированы для производителя устройства.

Если отсканированное устройство соответствует этим требованиям, все модули, из которых были получены данные, будут отображены, чтобы дать вам возможность выбрать, какой из них создавать, а какой нет.

Эти модули будут отображаться организованными в блоки в зависимости от группы, к которой принадлежит создавший их компонент *помощника*.

Все блоки сначала будут показаны в сжатом виде для облегчения визуализации, таким образом, они могут быть развернуты для изменения выбора или данных. Кроме того, в каждом блоке, где были отмечены модули для создания, вы увидите информативный значок, указывающий на это.



Если мы развернем блок, мы сможем выбрать, какие модули добавить, а какие нет, а также

изменить название, описание или пороговые значения каждого модуля в отдельности.

Module Name	Type	Description	Warning			Critical			Current value
			Min.	Max.	Inv.	Min.	Max.	Inv.	
CPU User (%)	SNMP DATA	The percentage of CPU time spent processing user-level code, calculated over the last minute	80.00	90.00	<input type="checkbox"/>	90.00	0.00	<input type="checkbox"/>	4 % <input checked="" type="checkbox"/>
CPU System (%)	SNMP DATA	The percentage of CPU time spent processing system-level code, calculated over the last minute	80.00	90.00	<input type="checkbox"/>	90.00	0.00	<input type="checkbox"/>	3 % <input checked="" type="checkbox"/>
CPU Idle (%)	SNMP DATA	The percentage of CPU time spent idle, calculated over the last minute	0.00	0.00	<input type="checkbox"/>	0.00	0.00	<input type="checkbox"/>	89 % <input type="checkbox"/>
Load average - Load-1	SNMP DATA	The 1, 5 or 15 minutes load average	0.00	0.00	<input type="checkbox"/>	0.00	0.00	<input type="checkbox"/>	0.38 <input type="checkbox"/>
Load average - Load-5	SNMP DATA	The 1, 5 or 15 minutes load average	0.00	0.00	<input type="checkbox"/>	0.00	0.00	<input type="checkbox"/>	0.35 <input type="checkbox"/>
Load average - Load-15	SNMP DATA	The 1, 5 or 15 minutes load average	0.00	0.00	<input type="checkbox"/>	0.00	0.00	<input type="checkbox"/>	0.33 <input type="checkbox"/>

Memory >

Other >

Disk devices >

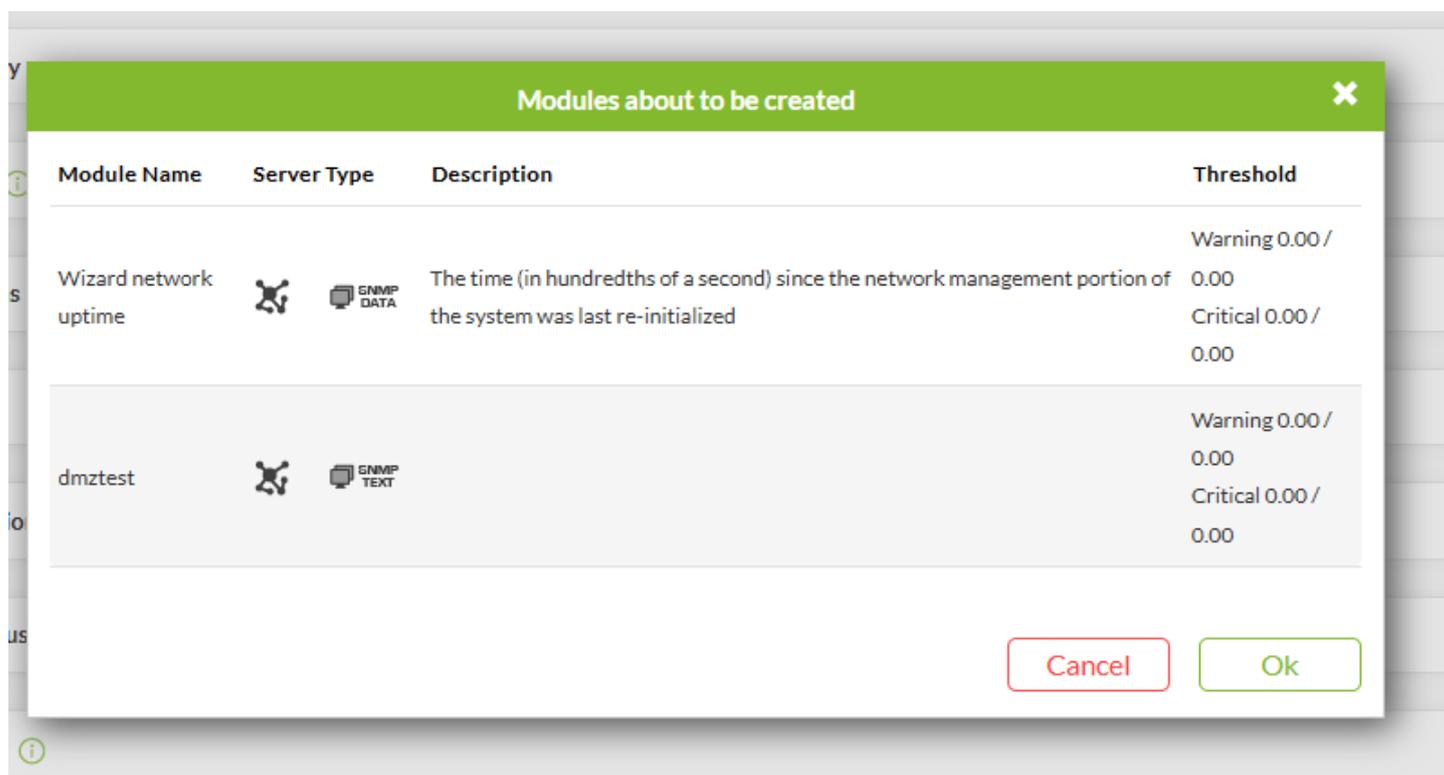
Storage >

Processes >

После нажатия кнопки *Create modules* появится сводный список выбранных модулей с их конфигурацией. В этом списке вы увидите модули, которые не могут быть созданы, либо потому что они уже существуют в агенте, либо потому что вы настроили 2 или более модулей с одинаковым именем в самом *wizard*.

Обратите внимание, что если значение модуля, взятое помощником *wizard*, имеет тип **инкрементный** или **абсолютно инкрементный**, это значение является не самим приращением, а опорным значением. Для получения инкрементного значения необходимо два показания, поэтому значение модуля будет показывать «ноль» до следующего снятия показаний.

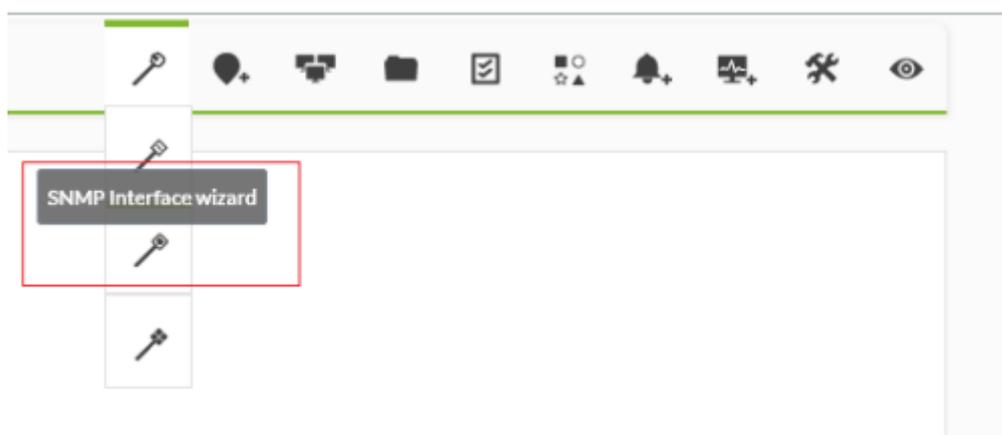
Прежде чем они будут добавлены в агент, вам будет предоставлена последняя возможность подтвердить создание этих модулей или отменить его и продолжить модификацию результата *wizard*.



После того, как создание модулей будет подтверждено, они будут повторно оценены по одному, на возможность их создания, чтобы избежать дублирования модулей в случае, если те же самые модули были созданы другими способами в течение выбранного периода.

Вы получите уведомление об успешном завершении процесса или о том, что не удалось создать какой-либо модуль.

SNMP Interfaces wizard



В *Помощнике Агентов* есть мастер SNMP, специально созданный для навигации по интерфейсам. Этот *Wizard* осуществляет навигацию по ветке SNMP IF-MIB::interfaces,

предлагая возможность создания нескольких модулей различных интерфейсов с множественным выбором. После выбора целевого IP, сообщества и т.д. система отправит SNMP-запрос к целевому устройству и заполнит форму для создания модуля.



Select all filtered interfaces Search _____



OperStatus UP



AdminStatus UP



dmz



mgmt



wan1



wan2



ha1



ha2



x1



x2



modem



ssl.root



lan



port9



port3



port12



port5



port7



port2



port1



Вы можете выбрать один или несколько интерфейсов из списка слева. Затем справа появятся общие для них элементы (Описание, Скорость, Входящий/Исходящий трафик...). Вы можете выбрать один или несколько элементов из комбинации и нажать Создать модули, чтобы создать выбранные модули для каждого интерфейса, выбранного в комбинации слева.

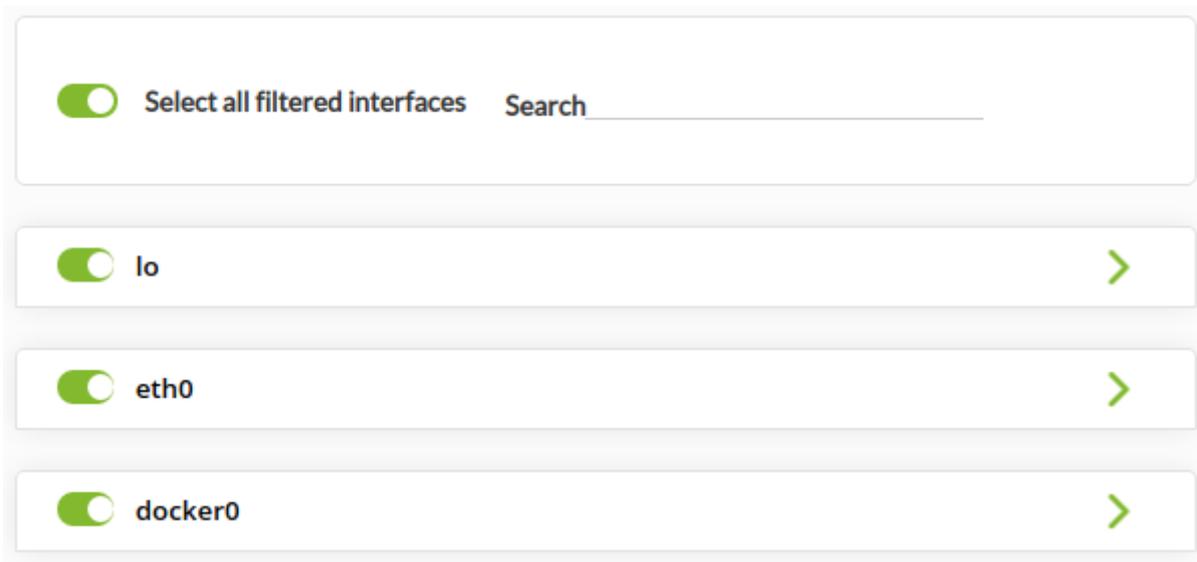
Для того чтобы помощник интерфейсов SNMP мог получить данные от устройства SNMP, устройство SNMP должно вернуть данные из ветви IF-MIB.

Вы увидите первый общий блок конфигурации для всех выбранных интерфейсов устройства с возможными модулями для добавления. Выбранные в этом блоке модули и их пороговые значения будут конфигурацией по умолчанию, которая будет добавлена для сетевых интерфейсов. Этот блок может быть отключен, чтобы не добавлять общий мониторинг в интерфейсы.

Add general monitoring for all selected interfaces

Module Name	Type	Module info	Warning			Critical			<input type="checkbox"/>
			Min.	Max.	Inv.	Min.	Max.	Inv.	
ifInOctets	SNMP INC	The total number of octets received on the interface, including framing characters	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="checkbox"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
ifOutOctets	SNMP INC	The total number of octets transmitted out of the interface, including framing characters	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="checkbox"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
ifOperStatus	SNMP DATA	The current operational state of the interface: up(1), down(2), testing(3), unknown(4), dormant(5), notPresent(6), lowerLayerDown(7)	<input type="text" value="3"/>	<input type="text" value="0"/>	<input type="checkbox"/>	<input type="text" value="2"/>	<input type="text" value="3"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
ifAdminStatus	SNMP DATA	The desired state of the interface: up(1), down(2), testing(3)	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="checkbox"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="checkbox"/>	<input type="checkbox"/>
ifInDiscards	SNMP INC	The number of inbound packets which were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="checkbox"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="checkbox"/>	<input type="checkbox"/>
ifOutDiscards	SNMP INC	The number of outbound packets which were chosen to be discarded even though no errors had been detected to prevent their being transmitted	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="checkbox"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="checkbox"/>	<input type="checkbox"/>
ifInErrors	SNMP INC	For packet-oriented interfaces, the number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol. For character-oriented or fixed-length interfaces, the number of inbound transmission units that contained errors preventing them from being deliverable to a higher-layer protocol	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="checkbox"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="checkbox"/>	<input type="checkbox"/>
ifOutErrors	SNMP INC	For packet-oriented interfaces, the number of outbound packets that could not be transmitted because of errors. For character-oriented or fixed-length interfaces, the number of outbound transmission units that could not be transmitted because of errors	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="checkbox"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="checkbox"/>	<input type="checkbox"/>
ifInUcastPkts	SNMP INC	The number of packets, delivered by this sub-layer to a higher (sub-)layer, which were not addressed to a multicast or broadcast address at this sub-layer	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="checkbox"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="checkbox"/>	<input type="checkbox"/>
ifOutUcastPkts	SNMP INC	The total number of packets that higher-level protocols requested be transmitted, and which were not addressed to a multicast or broadcast address at this sub-layer, including those that were discarded or not sent	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="checkbox"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="checkbox"/>	<input type="checkbox"/>
ifInMulticastPkts	SNMP INC	The number of packets, delivered by this sub-layer to a higher (sub-)layer, which were addressed to a multicast or broadcast address at this sub-layer	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="checkbox"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="checkbox"/>	<input type="checkbox"/>
ifOutMulticastPkts	SNMP INC	The total number of packets that higher-level protocols requested be transmitted, and which were addressed to a multicast or broadcast address at this sub-layer, including those that were discarded or not sent	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="checkbox"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="checkbox"/>	<input type="checkbox"/>

В нем есть специальный блок для каждого сетевого интерфейса, который можно выбрать, чтобы указать, что интерфейс должен контролироваться. Если в предыдущем блоке также был настроен общий мониторинг, то все отмеченные интерфейсы будут принимать эти конфигурации.



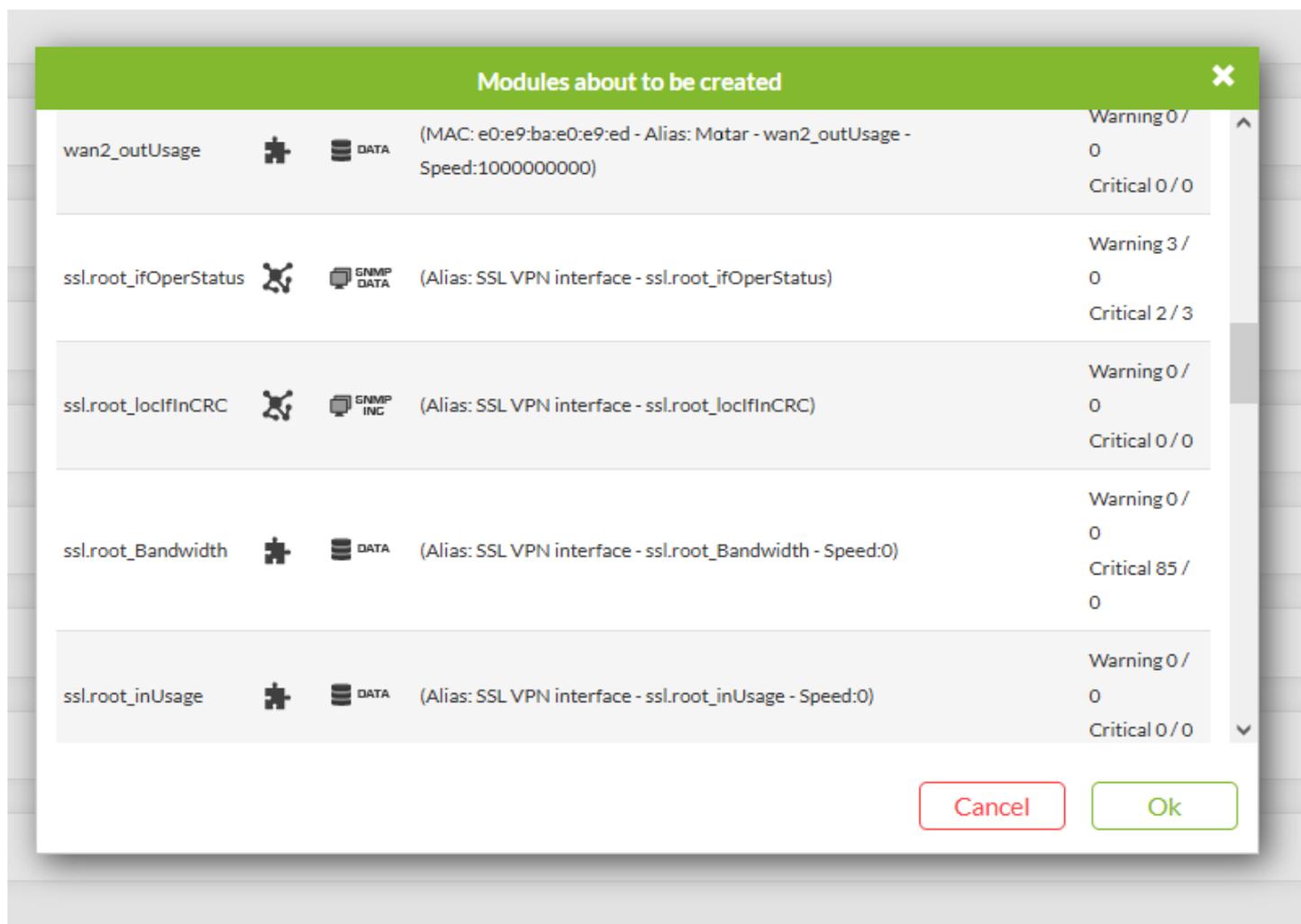
В каждом блоке интерфейса мы также можем указать специфические конфигурации для интерфейса, то есть добавить более специфические модули, которые не включены в общий блок мониторинга, или перезаписать эти конфигурации другой конфигурацией для данного случая. Вы также можете изменять названия и описания модулей для каждого конкретного случая. Необходимо, чтобы интерфейсный блок был помечен для мониторинга, чтобы конкретные конфигурации вступили в силу.

Module Name	Type	Description	Warning			Critical			Current value	Toggle
			Min.	Max.	Inv.	Min.	Max.	Inv.		
eth0_ifInOctets	SNMP INC	(MAC: b6:e1:fd:fe:ce:e6 - IP: 192.168.80.43 - eth0_ifInOctets)	0	0	<input type="checkbox"/>	0	0	<input type="checkbox"/>	1,325,509,35... bytes/s	<input type="checkbox"/>
eth0_ifOutOctets	SNMP INC	(MAC: b6:e1:fd:fe:ce:e6 - IP: 192.168.80.43 - eth0_ifOutOctets)	0	0	<input type="checkbox"/>	0	0	<input type="checkbox"/>	54,853,587 bytes/s	<input type="checkbox"/>
eth0_ifOperStatus	SNMP DATA	(MAC: b6:e1:fd:fe:ce:e6 - IP: 192.168.80.43 - eth0_ifOperStatus)	3	0	<input type="checkbox"/>	2	3	<input type="checkbox"/>	up(1)	<input type="checkbox"/>
eth0_ifAdminStatus	SNMP DATA	(MAC: b6:e1:fd:fe:ce:e6 - IP: 192.168.80.43 - eth0_ifAdminStatus)	0	0	<input type="checkbox"/>	0	0	<input type="checkbox"/>	up(1)	<input type="checkbox"/>
eth0_ifInDiscards	SNMP INC	(MAC: b6:e1:fd:fe:ce:e6 - IP: 192.168.80.43 - eth0_ifInDiscards)	0	0	<input type="checkbox"/>	0	0	<input type="checkbox"/>	0 packets/s	<input type="checkbox"/>
eth0_ifOutDiscards	SNMP INC	(MAC: b6:e1:fd:fe:ce:e6 - IP: 192.168.80.43 - eth0_ifOutDiscards)	0	0	<input type="checkbox"/>	0	0	<input type="checkbox"/>	0 packets/s	<input type="checkbox"/>
eth0_ifInErrors	SNMP INC	(MAC: b6:e1:fd:fe:ce:e6 - IP: 192.168.80.43 - eth0_ifInErrors)	0	0	<input type="checkbox"/>	0	0	<input type="checkbox"/>	0 packets/s	<input type="checkbox"/>
eth0_ifOutErrors	SNMP INC	(MAC: b6:e1:fd:fe:ce:e6 - IP: 192.168.80.43 - eth0_ifOutErrors)	0	0	<input type="checkbox"/>	0	0	<input type="checkbox"/>	0 packets/s	<input type="checkbox"/>
eth0_ifInUcastPkts	SNMP INC	(MAC: b6:e1:fd:fe:ce:e6 - IP: 192.168.80.43 - eth0_ifInUcastPkts)	0	0	<input type="checkbox"/>	0	0	<input type="checkbox"/>	1,021,165 packets/s	<input checked="" type="checkbox"/>
eth0_ifOutUcastPkts	SNMP INC	(MAC: b6:e1:fd:fe:ce:e6 - IP: 192.168.80.43 - eth0_ifOutUcastPkts)	0	0	<input type="checkbox"/>	0	0	<input type="checkbox"/>	323,207 packets/s	<input checked="" type="checkbox"/>
eth0_ifInNUcastPkts	SNMP INC	(MAC: b6:e1:fd:fe:ce:e6 - IP: 192.168.80.43 - eth0_ifInNUcastPkts)	0	0	<input type="checkbox"/>	0	0	<input type="checkbox"/>	0 packets/s	<input type="checkbox"/>
eth0_ifOutNUcastPkts	SNMP INC	(MAC: b6:e1:fd:fe:ce:e6 - IP: 192.168.80.43 - eth0_ifOutNUcastPkts)	0	0	<input type="checkbox"/>	0	0	<input type="checkbox"/>	0 packets/s	<input type="checkbox"/>

Сначала все блоки будут показаны в сжатом виде, чтобы облегчить визуализацию. Таким образом, их можно будет расширить, чтобы изменить выбранное или данные. Кроме того, в каждом блоке, где были отмечены модули для создания, вы увидите информативный значок, указывающий на это.

После нажатия кнопки *Create modules* появится сводный список выбранных модулей с их конфигурацией. В этом списке вы увидите модули, которые не могут быть созданы, либо потому что они уже существуют в агенте, либо потому что 2 или более модулей с одинаковым именем были настроены в самом wizard.

Несмотря на все внесенные изменения, перед их добавлением в агент будет последняя возможность подтвердить создание этих модулей или отменить его и продолжить модификацию результата работы помощника.



После того, как создание модулей будет подтверждено, они будут повторно оценены по одному, на возможность их создания, чтобы избежать дублирования модулей в случае, если те же самые модули были созданы другими способами в течение выбранного периода.

Мы получим уведомление, если процесс завершился успешно или, наоборот, если не удалось создать какой-либо другой модуль.

Удаленный мониторинг Windows с помощью WMI

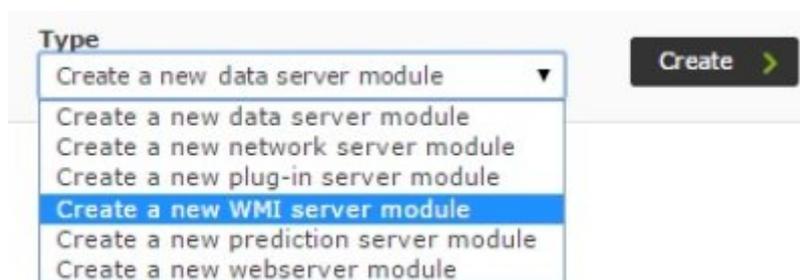
WMI - это технология, используемая в операционной системе Microsoft для получения удаленной информации с компьютеров под управлением Windows® она доступна начиная с версии Windows XP и заканчивая самыми последними версиями. WMI позволяет получать всевозможную информацию об ОС, приложениях и даже о программном обеспечении. Запросы WMI можно выполнять локально с помощью программного агента (вызывая API операционной системы) или удаленно. В некоторых системах удаленный доступ к WMI не активирован, и его необходимо активировать, чтобы иметь возможность получать консультации извне.

Необходимо включить компонент wmi_server в файле конфигурации сервера Pandora FMS.

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

Запросы выполняются на WQL, своеобразном языке SQL от Microsoft для запросов внутри операционной системы, и может быть выполнен любой запрос, который появляется в базе данных системы WMI.

Чтобы начать мониторинг с помощью WMI, сначала необходимо создать соответствующего агента, а затем щелкнуть на верхней вкладке модулей. (Modules). В ней выберите создать новый модуль WMI и нажмите на кнопку Create:



Специфические поля WMI требуют небольшого пояснения:

- Namespace: Пространство имен WMI; в некоторых запросах это поле отличается от пустой строки (по умолчанию), в зависимости от поставщика информации приложения, в котором

проводится мониторинг.

- Username: Имя пользователя-администратора или другого пользователя, имеющего привилегии для удаленного выполнения WMI-запросов.
- Password: Пароль.
- Key string: Необязательное, поле для сравнения со строкой, возвращаемой запросом, и если существует, модуль возвращает 1 или 0, вместо самой строки.
- Field number: Номер возвращаемого поля, начиная с 0 (запросы WMI могут возвращать более одного поля). В большинстве случаев это 0 или 1.
- WMI Query: WMI-запрос, аналогичный SQL-инструкции.

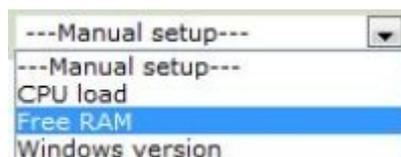
Некоторые примеры *WMI Query*:

```
SELECT LoadPercentage from Win32_Processor WHERE DeviceID = "CPU0"  
SELECT SerialNumber FROM Win32_OperatingSystem  
SELECT AvailableBytes from Win32_PerfRawData_PerfOS_Memory  
SELECT DiskWriteBytesPersec from Win32_PerfRawData_PerfDisk_PhysicalDisk WHERE  
name = "_Total"
```

Если вы не знаете точных параметров, вы можете выбрать один из параметров по умолчанию, включенных в базу данных Pandora FMS. Для этого выберите компонент модуля WMI:



Затем выберите проверку WMI из возможных:



Необходимая информация заполняется автоматически, за исключением имени пользователя и пароля. Обратите внимание, что вы должны ввести пользователя с правами администратора и свой пароль; в противном случае модуль не сможет вернуть никаких значений.:

Using module component ? Windows System Windows version

Name Disabled Module group General

Module parent

Type ?

Dynamic Threshold Interval ?  

Warning status ?
 Inverse interval

Critical status ?
 Inverse interval

FF threshold ? Change all statuses :
 Change each status : To 'normal' To 'warning' To 'critical'

Historical data

Target IP Namespace ?

Username Password

WMI query ?

Key string ? Field number ?

Версия Pandora FMS Enterprise имеет более 400 модулей удаленного мониторинга WMI для Windows, охватывающих все технологии:

- Active Directory®.
- BIOS.
- Информация о системе.
- Информация о Windows®.
- Принтеры.
- MSTDC.
- IIS.
- LDAP.
- Microsoft Exchange®.

Wizard WMI

Используется для навигации и создания модулей с WMI-запросами к определенному агенту. В *Wizard* агентов (вкладка в просмотре администрирования агента) щелкните на значок :



Вы должны указать имя пользователя и пароль с правами на выполнение WMI-запросов (или, в противном случае, администратора) на целевом сервере для выполнения первых WMI-запросов. Эта информация будет использована для создания модулей.

Target IP	<input type="text" value="gatomon.lab.artica.e"/>	Namespace ?	<input type="text"/>
Username	<input type="text" value="Administrator"/>	Password	<input type="text"/>
Server to execute command	<input type="text" value="Local console"/> ▼		

WMI Explorer >

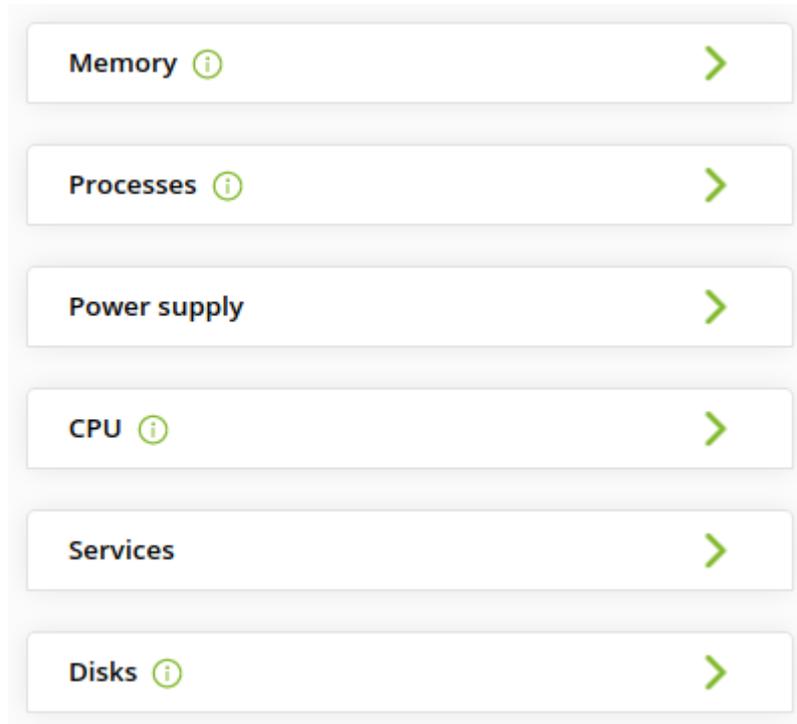
С помощью Wizard WMI можно создавать модули различных типов информации WMI:

- Службы: Булевы (логические) мониторы будут созданы в нормальном состоянии, если служба запущена, и в необработанном состоянии, если служба остановлена.
- Процессы: Мониторы процессов будут получать информацию только тогда, когда процесс активен. В противном случае они попадут в неизвестное состояние.
- Свободное пространство на диске
- Компоненты WMI: В этом случае выберите между компонентами WMI, зарегистрированными в

системе (Администрирование; Управление модулями; Управление модулями; Сетевые компоненты).

Вы должны были зарегистрировать и включить в Pandora компоненты мастера WMI: таким образом, будут показаны все модули, из которых вы могли бы получить данные, чтобы иметь возможность создать их или нет.

Эти модули будут отображаться по блокам на основе группы, к которой принадлежит создавший их компонент помощника.



Все блоки сначала будут показаны в сжатом виде для облегчения визуализации, а потом они могут быть развернуты для изменения выбранных модулей или данных. Кроме того, в каждом блоке, где были отмечены модули для создания, вы увидите информативный значок, указывающий на это.

Если мы развернем блок, мы сможем выбрать, какие модули добавить, а какие нет, а также изменить название, описание или пороговые значения каждого модуля в отдельности.



После нажатия кнопки *Create modules* появится список с кратким описанием выбранных модулей с их конфигурацией. В этом списке вы увидите модули, которые не могут быть созданы, либо потому что они уже существуют в агенте, либо потому что вы настроили 2 или более модулей с одинаковым именем в самом *wizard*.

Несмотря на все внесенные изменения, останется последняя возможность подтвердить создание этих модулей или отменить его и продолжить изменение результата работы *wizard*.

Modules about to be created			
Module Name	Server Type	Description	Threshold
WMI total RAM used (%)	 	Percentage of physical memory currently used	Warning 80.00 / 90.00 Critical 90.00 / 0.00
WMI Number of processes	 	Number of process contexts currently loaded or running on the operating system	Warning 0.00 / 0.00 Critical 0.00 / 0.00
WMI CPU0 usage (%)	 	Load capacity of each processor, averaged to the last second	Warning 80.00 / 90.00 Critical 90.00 / 0.00
WMI disk C: used (%)	 	Space percentage used on the logical disk	Warning 80.00 / 90.00 Critical 90.00 / 0.00

После того, как создание модулей будет подтверждено, они будут повторно оценены по одному, на возможность их создания, чтобы избежать дублирования модулей в случае, если те же самые модули были созданы другими способами в течение выбранного периода.

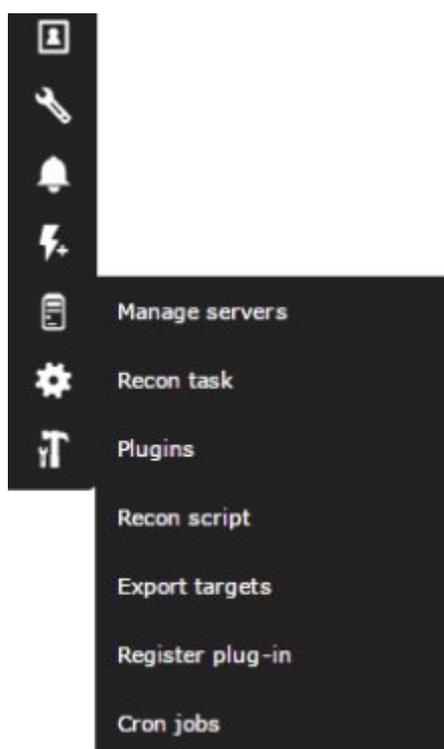
Помощник уведомит вас об успешном завершении процесса или о том, что не удалось создать какой-либо другой модуль.

Мониторинг с помощью плагинов удаленного сервера

plugin remoto - это скрипт (*script*) или исполняемый файл, который поддерживает параметры и возвращает одно и только одно значение. Результатом может быть число, булево значение (0 = ошибка, 0 <> ОК) или текстовая строка. Удаленный *plugin* обычно позволяет осуществлять параметры ввода. По умолчанию установлено и готово к использованию несколько серверных *plugins*, и пользователь всегда может добавить те, которые ему нужны.

Существует два вида удаленного *плагина*: стандартный и тип **Nagios**. Разница заключается главным образом в том, что тип Nagios отвечает уровнем ошибки (*error level*) и дополнительно, опционально, описательной строкой.

Администрирование плагинов с удаленным управлением



Нажмите на Управление серверами, а затем Управление плагинами, откроется новое окно:

Plug-ins registered in Pandora FMS

Name	Type	Command	Op.
DNS Plugin	Standard	/usr/share/pandora_server/util/plugin/dns_plugin.sh	 
IPMI Plugin	Standard	/usr/share/pandora_server/util/plugin/ipmi-plugin.pl	 
MySQL Plugin	Standard	/usr/share/pandora_server/util/plugin/mysql_plugin.sh	  
Packet Loss	Standard	/usr/share/pandora_server/util/plugin/packet_loss.sh	  
SMTP Check	Standard	/usr/share/pandora_server/util/plugin/SMTP_check.pl	 
SNMP remote	Standard	perl /usr/share/pandora_server/util/plugin/snmp_remote.pl	 
UDP port check	Standard	/usr/share/pandora_server/util/plugin/udp_nmap_plugin.sh	 

[Add >](#)

Щелчок на одном из них или создание нового откроет следующее диалоговое окно:

PLUG-IN UPDATE ?

General

Name

Plug-in type

Max. timeout ★

Description

Plug-in type позволяет установить, является ли он стандартным или типа Nagios. Max. timeout для установки времени ожидания выполнения, *особое внимание следует уделить этому значению, так как оно должно покрывать достаточно времени для выполнения, иначе мы не получим никакого значения.*

При выполнении плагина есть три резервных значения: сервера, плагина и значение модуля. Значение сервера преобладает над остальными, а на втором месте - значение плагина. При значениях *timeout* сервера в 10 секунд, плагина в 20 и модуля с этим плагином в 30, максимальное время ожидания выполнения этого модуля составит 10 секунд.

Поле описания очень важно, так как оно будет видно в пользовательском интерфейсе плагина, выберите короткую и понятную надпись. На следующем примере показано практическое использование

Plugin ?

Target IP

Port

Основные значения конфигурации:

Command

Plug-in command 

Plug-in parameters 

Command preview `/usr/share/pandora_server/util/plugin/udp_nmap_plugin.sh -t _field1_ -p _field2_`

- Команда Plug-in: Путь где размещается *плагин*, по умолчанию в каталоге `/usr/share/pandora_server/util/plugin/`. Если вы используете собственные *плагины*, убедитесь, что у вас есть разрешения на выполнение (`chmod 755`).
- Параметры Plug-in. Позволяет устанавливать отдельные параметры с пробелами в дополнение к макрополям `_field1_ _field2_ ... _fieldN_`. Эти макросы будут отображаться как текстовые поля в конфигурации модуля, чтобы пользователь мог абстрагироваться от сложности использования модуля типа *плагин*. Это позволяет пользователю заполнить параметры вызова *скрипта* без необходимости знать, как он работает или как его вызвать.

Каждый макрос имеет три поля:

Parameters of macros 

Description (`_field1_`) **Default value** (`_field1_`)

Hide Value ★

Help (`_field1_`)

Description (`_field2_`) **Default value** (`_field2_`)

Hide Value ★

Help (`_field2_`)

Add macro  **Delete macro** 

Create 

- **Description:** Это метка, которая появляется рядом с полем в форме.
- **Default value:** Значение, присвоенное полю по умолчанию.
- **Help:** Пояснительный текст макроса, чтобы показать пример использования или лучше объяснить, для чего предназначено это поле.

Внутренние макросы

Аналогично предупреждениям, вы также можете использовать внутренние макросы в конфигурации *плагинов*. Поддерживаются следующие макросы:

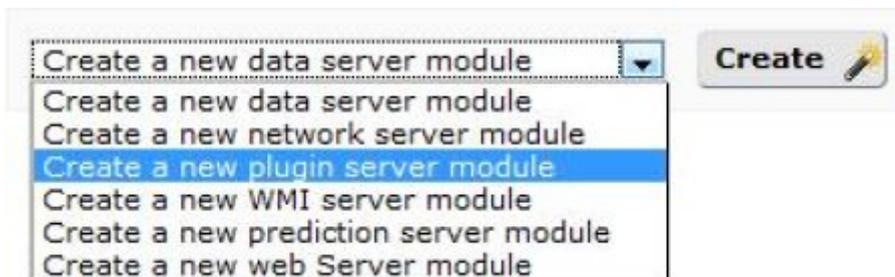
- `_agent_o_agentalias_>` Псевдоним агента, к которому принадлежит модуль.
- `_agentname_>` Имя агента, к которому принадлежит модуль.
- `_agentdescription_>` Описание агента, к которому принадлежит модуль.
- `_agentstatus_>` Текущий статус агента.
- `_address_>` Адрес агента, которому принадлежит модуль.
- `_module_>` Название модуля.
- `_modulegroup_>` Имя группы модулей.
- `_moduledescription_>` Описание модуля.
- `_modulestatus_>` Статус модуля.
- `_moduletags_>` Этикетки (*tags*) связанные с модулем.
- `_id_agent_>` ID агента, полезен для создания прямого URL или перенаправления на Консоль Pandora FMS.
- `_id_module_>` ID модуля.
- `_policy_>` Имя политики, к которой принадлежит модуль, если таковая установлена.
- `_interval_>` Интервал выполнения модуля.
- `_target_ip_>` IP-адрес назначения модуля.
- `_target_port_>` Порт назначения модуля.
- `_plugin_parameters_>` Параметры *плагина* модуля.
- `_email_tag_>` электронные письма, связанные с *тегами* модулей.

Удаленный плагин в системе

```
#!/bin/bash
# This is called like -p xxx -t xxxx
HOST=$4
PORT=$2
nmap -T5 -p $PORT -sU $HOST | grep open | wc -l
```

Этот *плагин* для GNU/Linux принимает два параметра, UDP порт для проверки `-p` и адрес назначения `-sU`. При регистрации *плагина* мы определили два макроса, один для порта, другой для IP, чтобы при создании модуля типа *плагин* пользователи отображали только эти параметры.

После регистрации *плагина* для его использования в агенте необходимо создать модуль типа *plugin server*.. Нажмите на на верхнюю вкладку модулей (Modules). В ней выберите создать новый сетевой модуль и нажмите на кнопку Create (создать):



Укажите IP-адрес Target IP и порт Port, где будет проводиться анализ, выберите тип модуля Generic numeric для сбора числового значения и заполните остальные поля, если это необходимо.

localhost.localdomain - Modules

Using module component ? --Manual setup--

Name: UDP port check Disabled

Type ? : Generic numeric Module group : General ▼

Warning status ? : Min. 0 Max. 0 Inverse interval Critical status ? : Min. 0 Max. 0 Inverse interval

FF threshold ? : All states changing : 0 Each state changing : To 'normal' To 'warning' To 'critical'

Historical data :

Plug-in ? : UDP port check Check a remote UDP port (by using NMAP). Use IP address and Port options.

Target IP : localhost

Port : 20

> Advanced options
> Custom macros ?
> Module relations

Create

После завершения нажмите на кнопку Create.



Пример #1: Модуль удаленного плагина для MySQL

MySQL - это механизм базы данных, для которого Pandora FMS создала *plugin* по умолчанию, настраиваемый каждым клиентом для своих пользователей. Для этого перейдите в Administration → Manage servers → plugins и добавьте новый подключаемый модуль для MySQL:

PLUGIN REGISTRATION

General

Name MySQL Plugin

Plugin type Standard

Max. timeout 15 seconds



Description

Samples:

```
./mysql_plugin.sh -u root -p none -s localhost -q Com_select
./mysql_plugin.sh -u root -p none -s localhost -q Com_update
./mysql_plugin.sh -u root -p none -s localhost -q Connections
./mysql_plugin.sh -u root -p anypass -s 192.168.50.24 -q Innodb_rows_read
```

Этот плагин обеспечивает четыре проверки, полностью прозрачные для пользователя (как вы увидите позже) с момента его запуска:

- -q Com_select: Количество запросов чтения *select*.
- -q Com_update: Количество запросов записи *update*.
- -q Connections: Количество соединений.
- -q Innodb_rows_read: Чтение рядов типа *Innodb*.

На следующем шаге введите местоположение *plugin* по умолчанию и четыре параметра для выполнения проверок, упомянутых выше:

Command

Plugin command `/usr/share/pandora_server/util/plugin/mysql_plugin.sh`



Plugin parameters `-s_field1_ -u_field2_ -p_field3_ -q_field4_`

Command preview `/usr/share/pandora_server/util/plugin/mysql_plugin.sh -s_field1_ -u_field2_ -p_field3_ -q_field4_`

Конфигурация первого и второго параметров (IP-адрес и имя пользователя):

Macro parameters

Description (_field1_)	IP address	Default value (_field1_)
Hide value 	<input type="checkbox"/>	
Help (_field1_)	IP address	

Description (_field2_)	Username	Default value (_field2_)
Hide value 	<input type="checkbox"/>	
Help (_field2_)	Username to access to database	

Создайте модуль в агенте устройства, на котором установлена Pandora FMS, его имя будет `MySQL Connections`, используя в качестве плагина `MySQL`, в качестве IP `localhost`, в качестве пользователя `pandora`, в качестве пароля - пароль базы данных Pandora FMS и слово для проверки будет `Connections`.

Создаваемый модуль будет выглядеть следующим образом:

Plugin ? MySQL Plugin

```

./mysql_plugin.sh -u root -p none -i localhost -q Can_select
./mysql_plugin.sh -u root -p none -i localhost -q Can_update
./mysql_plugin.sh -u root -p none -i localhost -q Connections
./mysql_plugin.sh -u root -p appsec -i 192.168.30.24 -q InnoDB_row_read

```

IP Address ? localhost

Username ? pandora

Password ? pandora

Query string ? connections

> Advanced options

> Custom macros

> Module relations

Create

После создания появляется в списке модулей типа *plugin* (в данном случае в ожидании инициализации):



Пример #2: Удаленный модуль плагина для SMTP-сервера

artica - Modules

Using module component ? --Manual setup--

Name Artica mail server **Disabled**

Type ? Generic numeric **Module group** General ?

Warning status ? Min. 0 Max. 0 **Critical status** ? Min. 0 Max. 0 Inverse interval

FF threshold ? All states changing : 0 Each state changing : To 'normal' To 'warning' To 'critical'

Historical data

Plug-in ? SMTP Check

This plugin is used to send a mail to a SMTP server and check if works.

Parameters in the plugin:

IP Address - SMTP Server IP address
 User - AUTH login
 Pass - AUTH password
 Port - SMTP port (optional)

Optional parameters:

-d Destination email
 -f Email of the sender
 -a Authentication system. Could be LOGIN, PLAIN, CRAM-MD5 or DIGEST-MD

Этот плагин отправляет сообщение с помощью удаленного сервера, возвращает 1, если работает, и 0, если не работает (тип `generic_proc`). Обратите внимание на текст справки, который появляется для параметров и дополнительных параметров. (*Parameters in the plugin* и *Optional parameters*, правый нижний угол).

При использовании *плагина* в конфигурации модуля должны быть установлены следующие параметры:

Target IP	<input type="text" value="mail.artica.es"/>
Port	<input type="text" value="15"/>
Username	<input type="text" value="mail.artica.es"/>
Password	<input type="text" value="-d mail@artica.es -f pandora_check@rtica.es -a LOGIN"/>
Optional parameters	<input type="text"/>

> **Advanced options**
 > **Custom macros** ?
 > **Module relations**

Create 

Пример #3: Удаленный модуль plugin для DNS-сервера

artica - Modules












Using module component ? --Manual setup--

<p>Name <input type="text" value="Domain Check"/></p> <p>Type ? Generic numeric</p> <p>Warning status ?</p> <p>Min. <input type="text" value="0"/> Max. <input type="text" value="0"/> Inverse interval <input type="checkbox"/></p> <p>FF threshold ?</p> <p><input checked="" type="radio"/> All states changing : <input type="text" value="0"/> <input type="radio"/> Each state changing : To 'normal' <input type="text"/> To 'warning' <input type="text"/> To 'critical' <input type="text"/></p> <p>Historical data <input checked="" type="checkbox"/></p> <p>Plug-in ? DNS Plugin</p>	<p>Disabled <input type="checkbox"/></p> <p>Module group General</p> <p>Critical status ?</p> <p>Min. <input type="text" value="0"/> Max. <input type="text" value="0"/> Inverse interval <input type="checkbox"/></p> <p><small>This plugin is used to check if a specific domain return a specific IP address, and to check how time (miliseccs) takes the DNS to answer. Use IP address parameter to specify the IP of your domain. Use these custom parameters for the other parameters:</small></p> <p><small>-d domain to check (for example pandorafms.com) -s DNS Server to check (for example 8.8.8.8)</small></p> <p><small>Optional parameters:</small></p> <p><small>-t Do a DNS time response check instead DNS resolve test</small></p>
---	--

Этот *плагин* возвращает IP-адрес домена, запрошенного к определенному DNS, возвращает

1 в случае работы и 0 в случае неудачи (тип данных `generic_proc`).

Target IP	<input type="text" value="68.154.54.146"/>
Domain to check ★	<input type="text" value="artica.es"/>
DNS Server to check ★	<input type="text" value="8.8.8.8"/>
Optional parameters	<input type="text"/>

› Advanced options
› Custom macros ?
› Module relations

Create 

Еще одним дополнительным мониторингом может быть проверка того, действительно ли все IP-адреса, возвращенные DNS, принадлежат запрашиваемому домену; это достигается путем сравнения с предыдущим и заранее определенным диапазоном IP-адресов.

Макросы пользовательских полей для удаленного мониторинга

При конфигурировании нескольких удаленных модулей необходимость несколько раз вводить информацию об одном и том же агенте может быстро стать монотонной (например, строка SNMP-сообщества). Макросы пользовательских полей позволяют вам использовать **пользовательские поля агента** в качестве макросов для определенных опций конфигурации модуля.

В следующем примере мы создадим сетевой компонент SNMP, который можно будет повторно использовать между агентами с разными строками SNMP-сообщества:

- В консоли Pandora FMS перейдите в раздел Resources > Custom fields и определите новое настраиваемое поле, в котором будет храниться строка сообщества SNMP. Запишите свой ID, поскольку впоследствии он станет частью макроса, и введите строку сообщества с соответствующим значением в агентах SNMP.

PANDORAFMS
ENTERPRISE

Pandora FMS
the Flexible Monitoring System

Enter keywords to search 

      (admin) 

Agent custom field manager



SUCCESS

Custom field successfully created

Total items: 11

ID	Field	Display up front 	Actions
1	Serial Number		 
2	Department		 
3	Additional ID		 
4	eHorusID		 
5	vmware_vcenter_ip		 
6	vmware_datacenter		 
7	vmware_user		 
8	vmware_pass		 
9	vmware_type		 
10	vmware_parent		 
11	SNMP Community		 

Total items: 11

Create field 

- Затем создайте **сетевой компонент SNMP** и введите `_agentcustomfield_<n_>` в качестве строки сообщества SNMP, где `n` - идентификатор пользовательского поля (в данном примере `_agentcustomfield_11_>`).

- Наконец, настройте модуль с помощью **сетевой компонент**, который вы только что создали. Модуль начнет работать автоматически.

Макросы пользовательских полей работают с модулями типа SNMP, WMI, *плагины* и инвентарь. Они могут использоваться в независимых модулях, сетевых компонентах и модулях политики.

Другой пример: для модуля типа WMI можно определить два новых пользовательских поля для хранения имени пользователя и пароля и использовать соответствующие макросы в определении модуля:

Удаленное выполнение помощников и сетевых тестов (Exec Server)

Только для серверов PFMS, установленных на GNU/Linux.

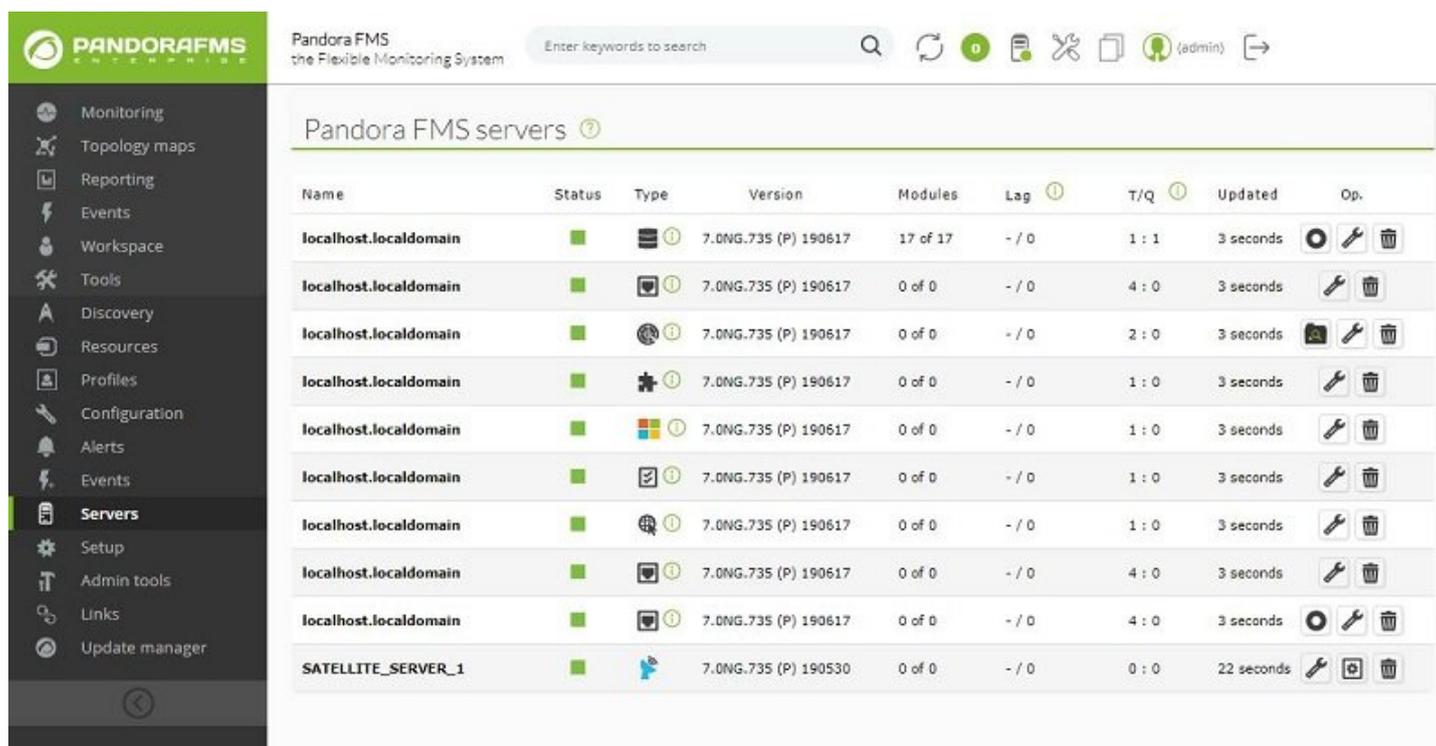
Эта функциональность позволяет выполнять некоторые действия на удаленных серверах Pandora FMS из консоли Pandora FMS. Таким образом, вы можете использовать SNMP-помощника агента, браузер MIB и *event responses* с удаленного сервера в дополнение к возможности делать это с сервера, на котором находится консоль. Внутри он работает через выполнение удаленных SSH-команд с консоли Pandora FMS на включенные серверы, называемые Exec Server. Это могут быть **Серверы Pandora FMS** или **спутниковые серверы**.

Конфигурация

В уже созданном Логическом Агенте с включенной удаленной конфигурацией устанавливается, что пользователь (например, «arache») с помощью пары созданных цифровых ключей (открытого и закрытого) может получить доступ к удаленному устройству, на котором размещен и настроен открытый ключ. По завершении SSH-соединение для автоматизированных процессов мониторинга уже будет настроено.

Без включенной функции удаленной конфигурации вы не сможете создавать модули Satellite с помощью помощников (*wizards*).

1. Из списка серверов Pandora FMS выберите один для работы в качестве Exec Server и отредактируйте его:



Name	Status	Type	Version	Modules	Lag	T/Q	Updated	Op.
localhost.localdomain	■	■	7.0NG.735 (P) 190617	17 of 17	- / 0	1 : 1	3 seconds	⏸️ 🔧 🗑️
localhost.localdomain	■	■	7.0NG.735 (P) 190617	0 of 0	- / 0	4 : 0	3 seconds	🔧 🗑️
localhost.localdomain	■	■	7.0NG.735 (P) 190617	0 of 0	- / 0	2 : 0	3 seconds	📺 🔧 🗑️
localhost.localdomain	■	■	7.0NG.735 (P) 190617	0 of 0	- / 0	1 : 0	3 seconds	🔧 🗑️
localhost.localdomain	■	■	7.0NG.735 (P) 190617	0 of 0	- / 0	1 : 0	3 seconds	🔧 🗑️
localhost.localdomain	■	■	7.0NG.735 (P) 190617	0 of 0	- / 0	1 : 0	3 seconds	🔧 🗑️
localhost.localdomain	■	■	7.0NG.735 (P) 190617	0 of 0	- / 0	1 : 0	3 seconds	🔧 🗑️
localhost.localdomain	■	■	7.0NG.735 (P) 190617	0 of 0	- / 0	4 : 0	3 seconds	🔧 🗑️
localhost.localdomain	■	■	7.0NG.735 (P) 190617	0 of 0	- / 0	4 : 0	3 seconds	⏸️ 🔧 🗑️
SATELLITE_SERVER_1	■	■	7.0NG.735 (P) 190530	0 of 0	- / 0	0 : 0	22 seconds	🔧 ⚙️ 🗑️

2. Установите флажок в поле Exec Server, введите порт и IP-адрес сервера, на котором будут запускаться нужные команды. Эту опцию может быть настроена на Network Server и/или Satellite Server.

The screenshot shows the Pandora FMS web interface. The top navigation bar includes the Pandora FMS logo, the text 'Pandora FMS the Flexible Monitoring System', a search bar with the placeholder 'Enter keywords to search', and several utility icons. A left sidebar menu lists various system components: Monitoring, Topology maps, Reporting, Events, Workspace, Tools, Discovery, Resources, Profiles, Configuration, Alerts, Events, Servers (highlighted), Setup, Admin tools, Links, and Update manager. The main content area is titled 'Update server' and displays configuration details for a server named 'SATELLITE_SERVER_1'. The fields include: Name (SATELLITE_SERVER_1), IP Address (192.168.70.171), Description (Autocreated at startup), Type (Satellite), Execute server (checked), Port (99), and a status indicator for 'Check execution of server' (a green dot). An 'Update' button is located at the bottom right of the configuration area.

Поскольку на данном этапе конфигурация не была завершена, тест подключения будет неудачным.

3. Чтобы пользователь примера “apache” (или эквивалентный ему) мог иметь *shell*, необходимо включить сервер, на котором работает Консоль Pandora FMS. В файле `/etc/passwd` измените следующую строку, чтобы у пользователя был действительный shell:

```
apache:x:48:48:Apache:/var/www:/bin/bash
```

4. Будет создан журнал `.ssh` на пути `/var/www/` и предоставляться разрешения для пользователя “apache”:

```
mkdir /var/www/.ssh
chown apache /var/www/.ssh
```

5. Теперь он должен действовать как *root* чтобы создать два ключа:

```
su apache
ssh-keygen
```

6. Примите значения по умолчанию, нажав клавишу *Enter*, вы увидите примерно

изменены:

```
chown -R pandora_exec_proxy /home/pandora_exec_proxy/.ssh/
```

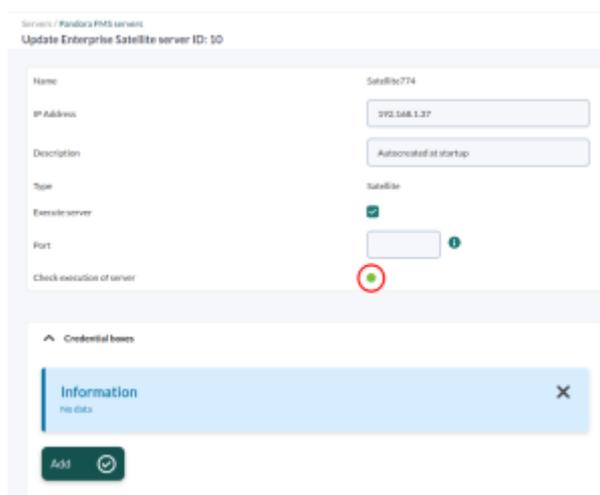
9. После создания этого пользователя, с устройства, на котором запущена консоль, под пользователем «apache» вручную выполните следующую команду для проверки возможности подключения без ввода пароля (замените «ip_address» на соответствующее значение из шага 2):

```
ssh pandora_exec_proxy@<ip_address>
```

10. Отредактируйте (в консоли) файл /etc/pass так, чтобы пользователь «apache» не мог начать сессию (он может быть вызван только, являясь *root*, см. шаг 5):

```
apache:x:48:48:Apache:/var/www:/sbin/nologin
```

11. Для завершения работы достаточно проверить конфигурацию в разделе редактирования прокси-сервера внутри консоли Pandora FMS, проверьте индикатор тестирования:



Использование функциональных возможностей Exec Server

После настройки, в проводнике MIB, в *помощниках* SNMP агента и в *event responses* вы можете выбрать, откуда запускать запрос: с локальной консоли или с настроенного Exec Server:

Аналогично для *Wizard WMI*, SNMP интерфейсов и *wizard* SNMP агента (кроме Satellite Server):

В зависимости от сервера, выбранного при запуске Помощника, будут созданы модули, адаптированные для сервера или Satellite Server. В последнем случае модули будут записаны в удаленный конфигурационный файл, чтобы они могли быть выполнены сервером.

Чтобы настроить новый *event response* с сервера Exec Server:

Pandora FMS
the Flexible Monitoring System

Enter keywords to search

Manage events - Responses

Name: Ping from Exec Server Group: All

Description:

Location: Modal window Size: Width (px) 620 Height (px) 500

Parameters:

Type: Command

Command: ping -c 5 _agent_address_ Server to execute command: SATELLITE_SERVER_1 (Satellite)

Create

Затем запустите его с какого-либо события:

Pandora FMS
the Flexible Monitoring System

Enter keywords to search

Module 'X1_iflnOctets' is going to UNKNOWN

General Details Agent fields Comments Responses

Change owner: None Update

Change status: New Update

Comment: Add comment

Delete event: Delete event

Custom responses: Ping from Exec Server Execute

Description:

Ping from Exec Server

> Executing command: ping -c 5 192.168.70.171

```

PING 192.168.70.171 (192.168.70.171) 56(84) bytes of data:
64 bytes from 192.168.70.171: icmp_seq=1 ttl=64 time=0.014 ms
64 bytes from 192.168.70.171: icmp_seq=2 ttl=64 time=0.019 ms
64 bytes from 192.168.70.171: icmp_seq=3 ttl=64 time=0.018 ms
64 bytes from 192.168.70.171: icmp_seq=4 ttl=64 time=0.021 ms
64 bytes from 192.168.70.171: icmp_seq=5 ttl=64 time=0.022 ms

--- 192.168.70.171 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4001ms
rtt min/avg/max/mdev = 0.014/0.018/0.022/0.006 ms

```

Мониторинг маршрутов

Pandora FMS по умолчанию предлагает мониторинг полных маршрутов между двумя точками сети, визуальнo отображая путь, по которому в любой момент может осуществляться связь между этими двумя точками.

Для использования этой системы вам необходимо:

- Программный агент в исходной точке пути, который мы хотим проанализировать.
- Достижение через ICMP из исходной точки.

Анализатор маршрутов Pandora FMS использует *plugin* агента для построения карты пути. Этот *plugin* Агента использует несколько методов для сбора информации, сообщая на сервер Pandora FMS структурированную информацию.

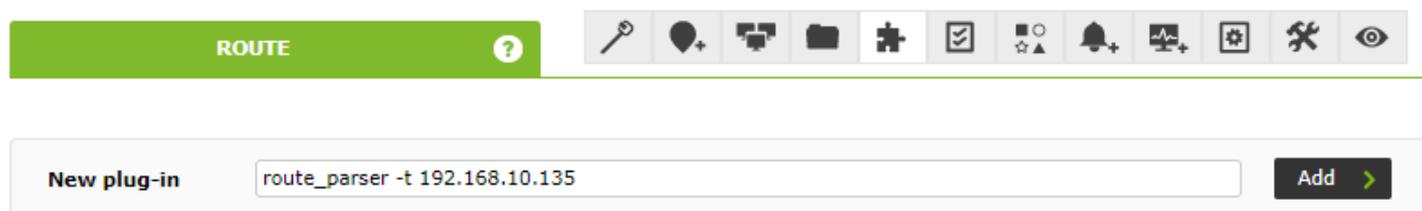
При желании, если вы хотите выполнять сканирование путей через Интернет, рекомендуется развернуть программу [MTR software](#) на устройстве источнике пути.

Конфигурация

Версия NG 715 или Выше

Зайдите на вкладку конфигурации плагинов в вашем агенте и добавьте следующую строку:

```
route_parser -t <direccion_objetivo>
```



Где <целевой адрес> может быть IP-адресом v4 или доменным именем FQDN.

- Наконец, активируйте выполнение *plugin*.

Примечание

Если вы используете Агента версии старше, чем NG 715, вы должны сначала:

- [Скачать plugin](#) для анализа пути библиотеки модулей.
- Передайте *плагин* Программному Агенту с помощью коллекций (или вручную скопируйте файл, см. следующий рисунок):

Sitio local:
 Sitio remoto: /usr/share/pandora_agent/plugins

Nombre de archivo	Tamaño de...	Tipo de archivo	Última modificación	Permisos	Pro
..					
route_parser	1.019.328	Archivo	26/10/2017 11:19:04		
grep_log_module	7.170	Archivo	19/07/2016 11:...	-rwxr-xr-x	par
inventory	11.973	Archivo	19/07/2016 11:...	-rwxr-xr-x	par
nagios_plugin_wrapp	2.484	Archivo	11/07/2017 17:...	-rwxr-xr-x	par
pandora_df	3.009	Archivo	11/07/2017 17:...	-rwxr-xr-x	par
pandora_df_free	2.346	Archivo	11/07/2017 17:...	-rwxr-xr-x	par
pandora_df_used	3.629	Archivo	11/07/2017 17:...	-rwxr-xr-x	par
pandora_mem	2.479	Archivo	11/07/2017 17:...	-rwxr-xr-x	par
pandora_mem_used	1.810	Archivo	11/07/2017 17:...	-rwxr-xr-x	par
pandora_netusage	509	Archivo	11/07/2017 17:...	-rwxr-xr-x	par
pandora_update	5.265	Archivo	19/07/2016 11:...	-rwxr-xr-x	par
route_parser	1.019.328	Archivo	26/10/2017 13:...	-rw-r--r--	roo
sockstat.sh	1.928	Archivo SH	11/07/2017 17:...	-rwxr-xr-x	par
top.sh	178	Archivo SH	11/07/2017 17:...	-rwxr-xr-x	par
who.sh	236	Archivo SH	11/07/2017 17:...	-rwxr-xr-x	par

Визуализация

После настройки системы и создания отчетов появится новая вкладка просмотра Агента с путем, по которому осуществлялась коммуникация для достижения цели:

Показ примера пути к устройству в сети, отличной от сети источника (LAN-подключения):

Global time: 4.2 ms



Просмотр примера пути к 8.8.8.8 (Google's DNS) (WAN-подключения)

Global time: 4.2 ms



[Вернуться в оглавление Pandora FMS](#)