Распространение топологии: Satellite Server

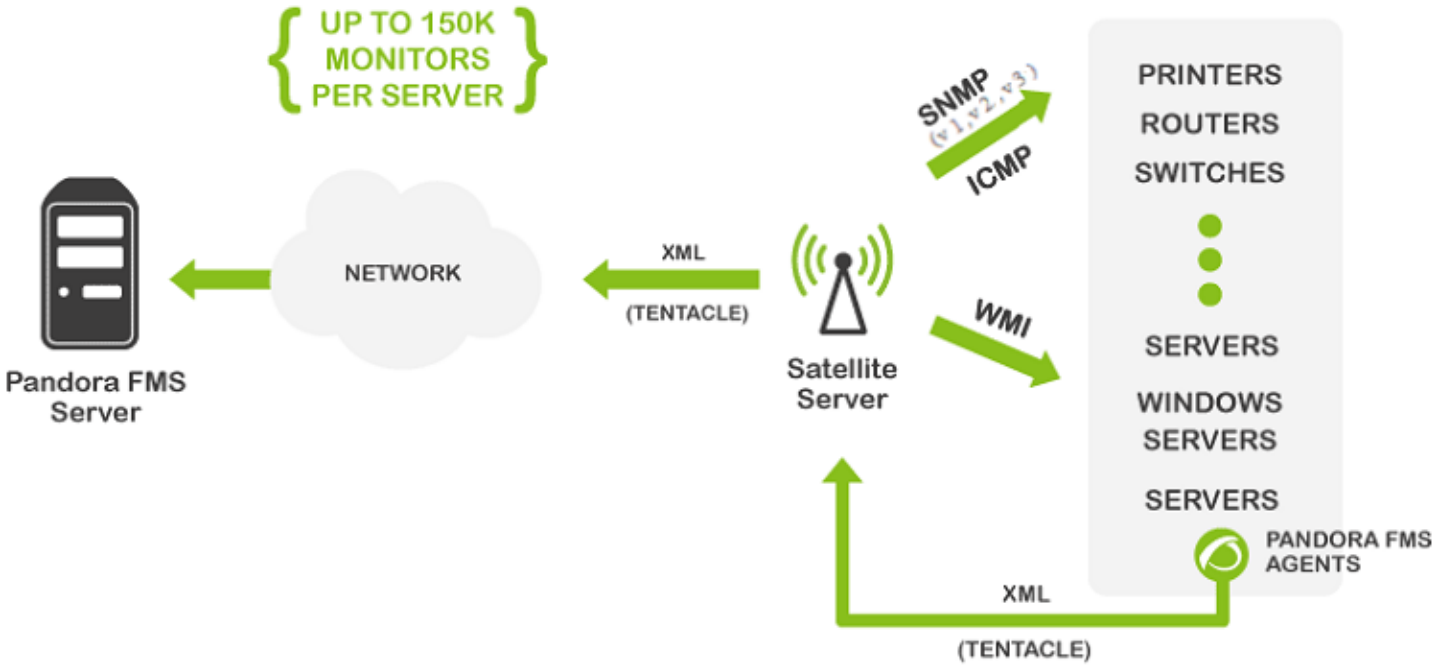
Распространение топологии: Satellite Server

Вернуться в оглавление Документации Pandora FMS

Satellite Server

Введение

Satellite Server используется для обнаружения и мониторинга удаленных сетей и оборудования, либо сетевых элементов (*routers*, *switches*, и т.д.) через SNMP или ICMP, либо серверов MS Windows® (через WMI) или Linux® (через SNMP). Это не «обычный» сервер, его скорее можно рассматривать как программный агент режим broker с расширенными функциями. Это особенно полезно для мониторинга удаленных сетей, недоступных с сервера Pandora FMS, и где мы также не можем установить программных агентов.



Satellite Server работает как в Windows®, так и в GNU/Linux® (рекомендуемая операционная система) и имеет некоторые особенности, которые делают его особенным, более чем подходящим для определенных сред.

- Он может выполнять сетевые тесты (ICMP, Latency и SNMP v1 и v2) с чрезвычайно высокой скоростью (500 проверок в секунду). Для SNMP v3 необходимо настроить учетные данные доступа, а из-за шифрования данных проверка будет менее быстрой.

- Он отправляет данные на сервер только каждые X секунд (по умолчанию 300), но может выполнять тесты латентности, ICMP и SNMP с меньшим интервалом (например, 30 секунд), чтобы, если состояние изменится, немедленно уведомлять сервер. Эти изменения состояния должны быть определены заранее, если тип модуля не является `*_proc` (например, сетевые интерфейсы или общие сетевые соединения).
- Это автономный сервер, он не требует подключения к базе данных Pandora FMS. Он отправляет все данные в формате XML, поэтому работает как независимый сервер, подобно программному агенту в режиме *брокера* или серверу экспорта.
- Он имеет механизм автообнаружения для SNMP и WMI, так что он создает обнаруженные агенты (по IP-адресу), обнаруживает динамические элементы (сетевые интерфейсы, хранилища) и отслеживает их автоматически.
- В системах Windows® он обнаруживает диски, процессор и память.
- В сетевых системах с SNMP он обнаруживает состояние интерфейса, входящий и исходящий трафик на интерфейс, а также имя системы.
- Авто-создаваемые модули могут быть изменены, как и любой другой модуль, путем управления агентом из консоли, как если бы это был обычный Агент (в разделе Массивные операции; Satellite).
- Вы можете создать агентов вручную, создав файл конфигурации агента в каталоге конфигурации Satellite Server (объяснение приведено ниже).

Версия NG 759 или более поздняя.

- Начиная с версии 759 NG, как сервер Satellite, так и сервер Enterprise Network Server поддерживают IPv6 во всех расширенных функциональных возможностях. Высокопроизводительный код, который ранее поддерживался только в IPv4, теперь применяется и в IPv6, расширяя существующие возможности *polling*.

Мощность

Максимальная мощностьSatellite Server полностью зависит от серверного оборудования, на котором он работает, и типа проверок, которые необходимо выполнить. В тестовой среде нам удалось выполнить 500 ICMP и SNMP проверок в секунду, но это сильно зависит от времени отклика удаленного устройства (время отклика в 10 миллисекунд - это не то же самое, что время отклика в 2 секунды). В идеальных теоретических условиях с помощью одного Satellite Server можно контролировать около 150 000 средств контроля. В реальных условиях около 50 000 модулей были протестированы в более или менее контролируемой среде (локальные сети) с помощью Satellite Server на компьютере с очень дискретным оборудованием (процессор Intel i5®, 2 ГГц, 4 ГБ ОЗУ).

Если имеется много модулей в критическом состоянии,
производительность может сильно пострадать..
Настроенный таймаут также необходимо учитывать,
поскольку за таймаут выполняется только одна

критическая проверка. Если у вас 1000 необработанных модулей, а таймаут установлен на 4 секунды, то для выполнения всех этих проверок одним потоком потребуется 4000 секунд.

Установка

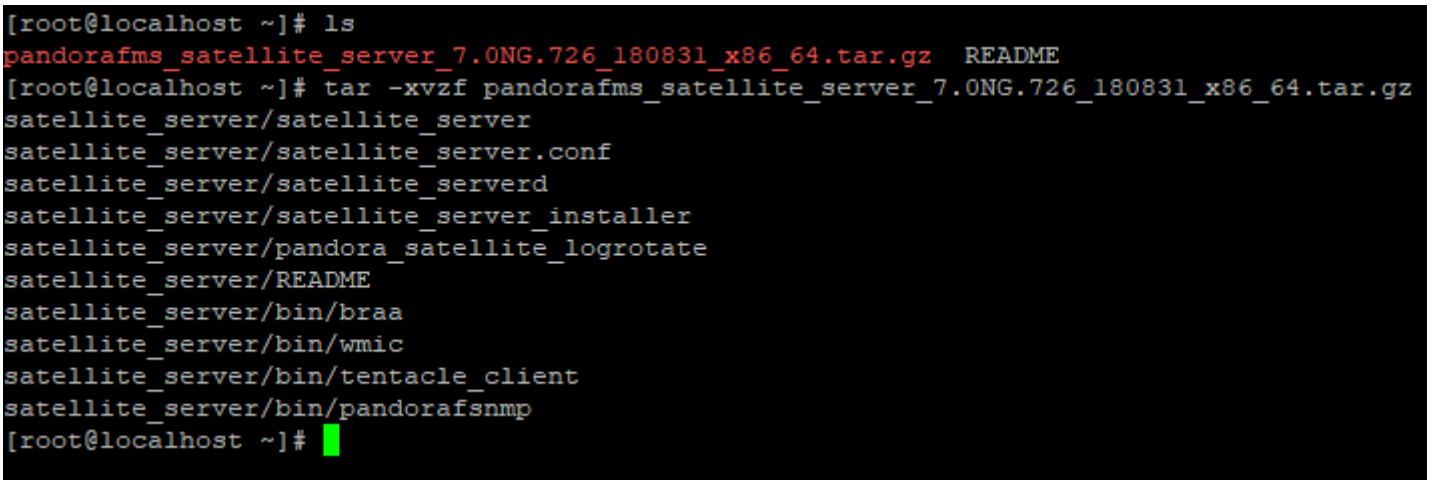
Satellite Server распространяется как tarball (GNU/Linux®) или `.exe` (Windows®), поэтому нет необходимости устанавливать Perl или какие-либо дополнительные библиотеки. Работа на версиях Windows® или Linux® ничем не отличается. В случае Windows® он устанавливается в качестве службы, а в случае Linux® - в качестве демона системы. Конфигурационный файл и спецификации обоих идентичны.

Версия Linux для Satellite Server зависит от внешних пакетов, которые указаны в соответствующем разделе данной документации.

Установка Satellite Server в Linux

Рекомендуемая операционная система GNU/Linux - CentOS.. После загрузки пакета, содержащего Satellite Server, необходимо перейти в папку загрузки с привилегиями root и распаковать двоичный файл:

```
tar -xvzf pandorafms_satellite_server_X.XNG.XXX_x86_64.tar.gz
```



После этого будет создана папка с именем `satellite_server`. Перейдите в эту папку, введя:

```
cd satellite_server/
```

Прежде чем приступить к установке, необходимо прояснить, какие фундаментальные

зависимости имеются у Satellite Server: Perl, Braa, Wmic, Fping и Nmap.

Установите Perl с помощью следующей команды:

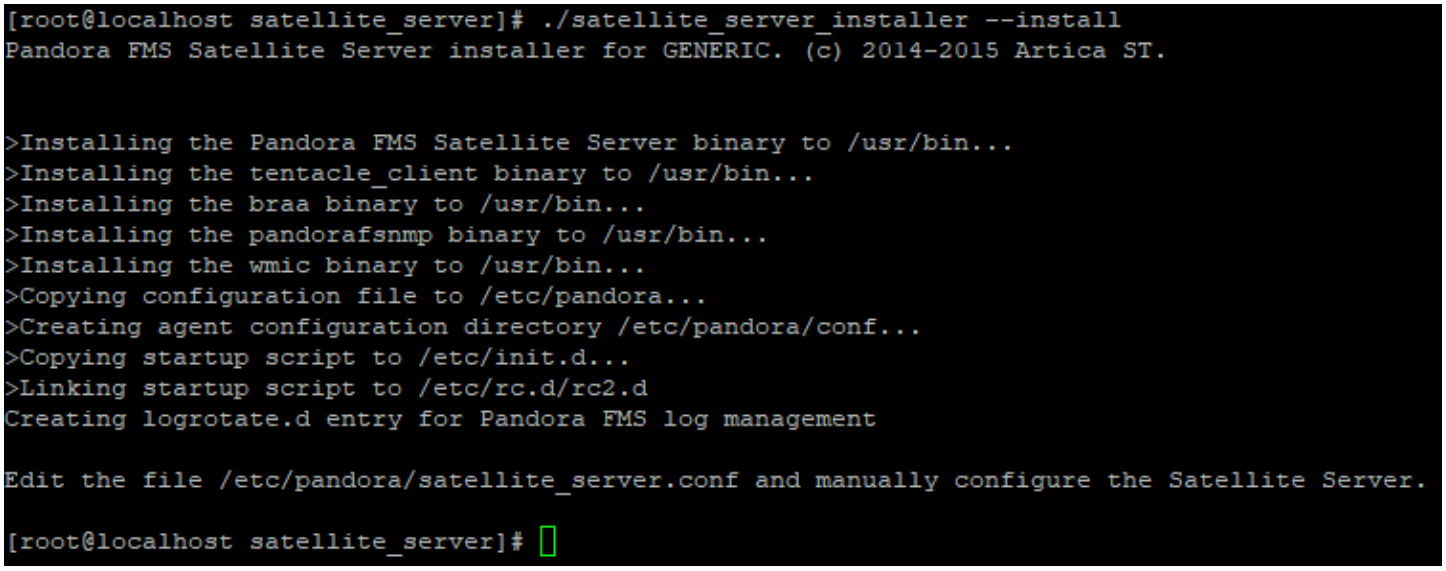
```
yum install perl
```

Зависимости Braa и Wmic прилагаются к программе установки. Fping и Nmap должны быть установлены отдельно:

```
yum install fping nmap
```

Чтобы установить сам Satellite Server, необходимо выполнить команду установки:

```
./satellite_server_installer --install
```



После завершения процесса необходимо отредактировать файл конфигурации satellite, расположенный по адресу:

```
/etc/pandora/satellite_server.conf
```

Текстовым редактором по умолчанию в CentOS является VIM. Найдите *токен* `pandora_license`, откомментируйте его и введите лицензию сервера Pandora FMS Enterprise. После этого вы можете сохранить файл и запустить службу, выполнив следующее:

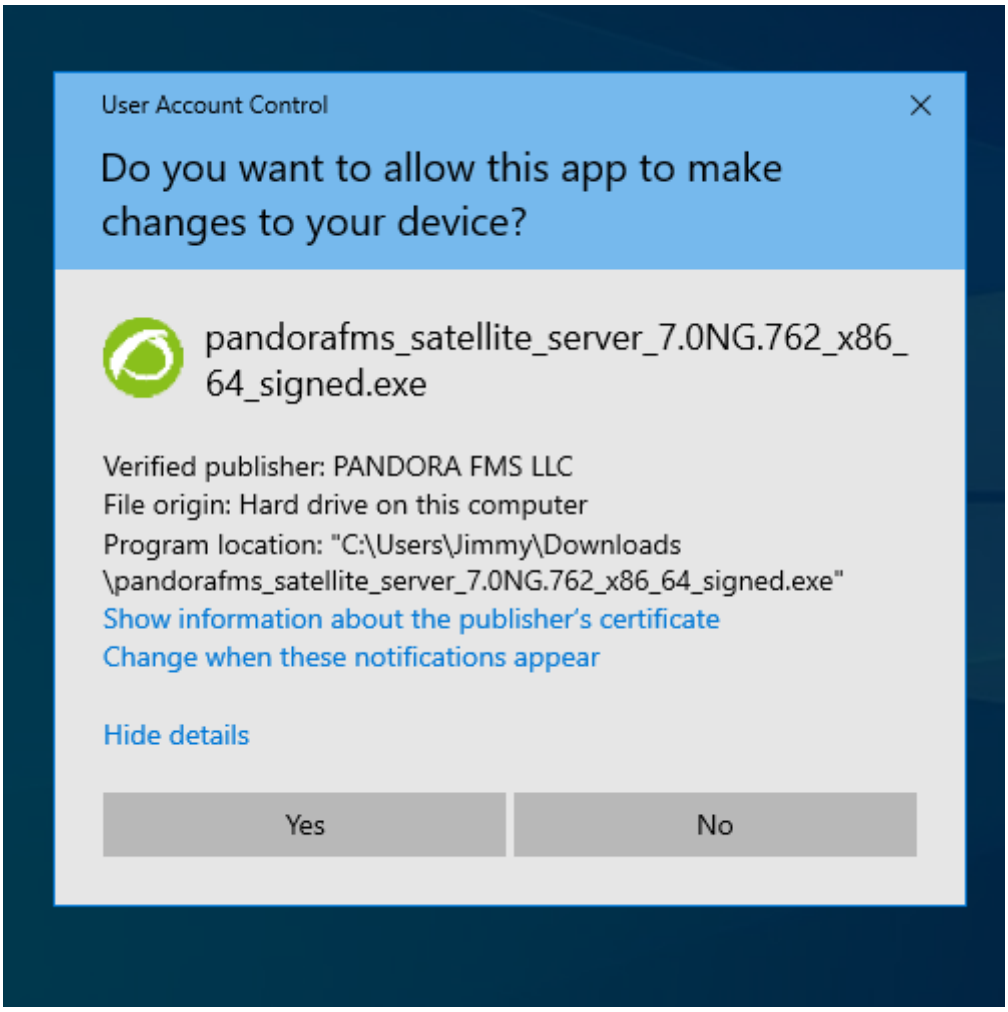
```
sudo /etc/init.d/satellite_serverd start
```

В случае любой ошибки или сбоя вы можете проверить файл журнала по адресу:

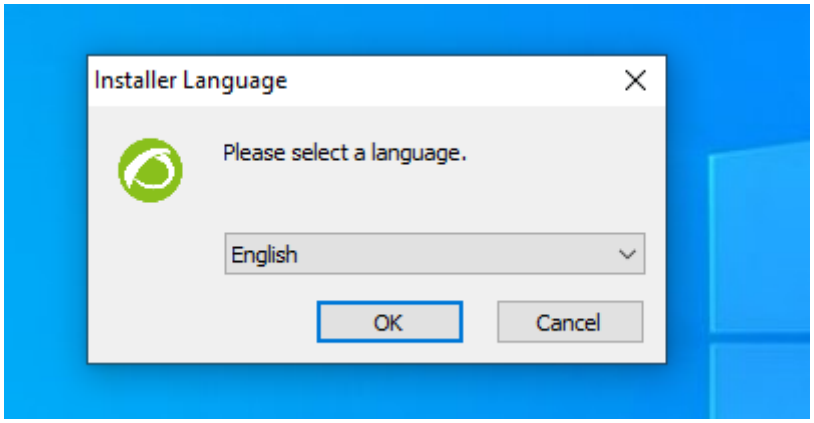
```
/var/log/satellite_server.log
```

Установка в Windows

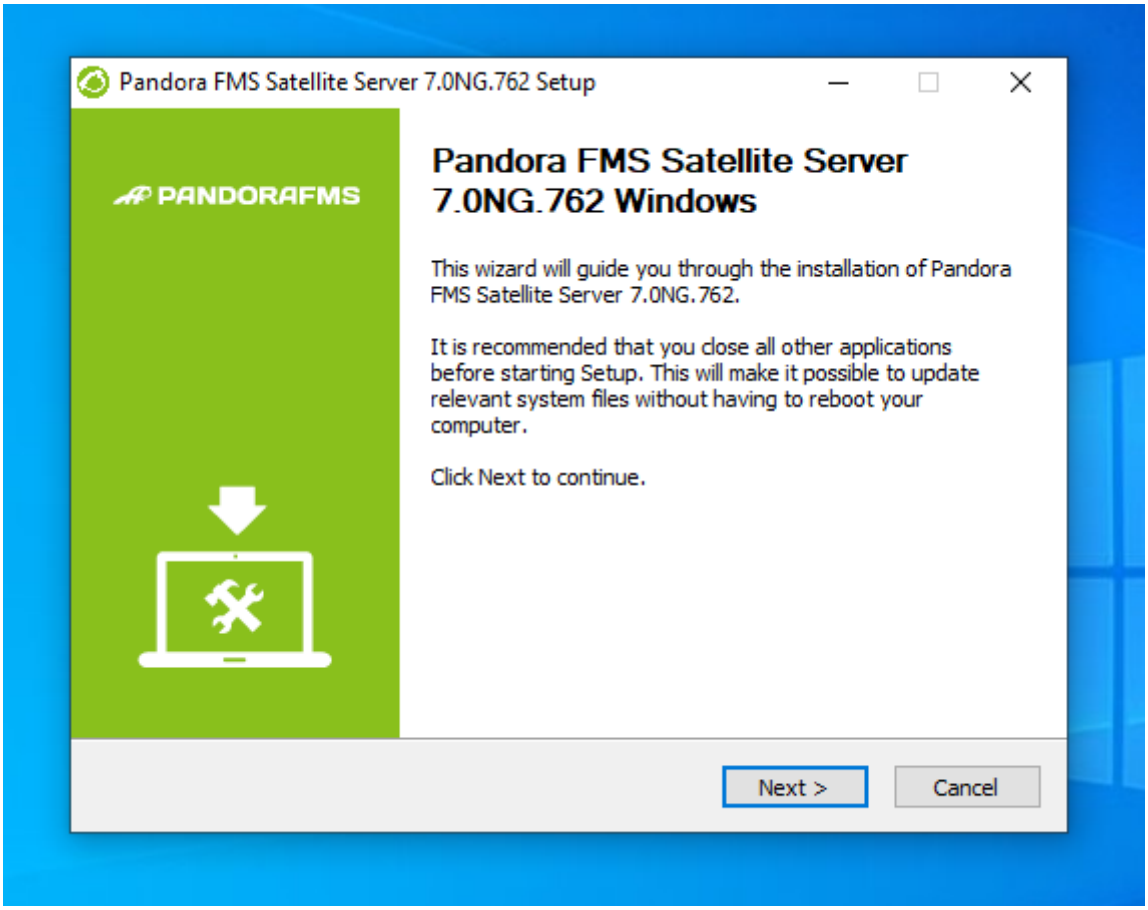
Запустите программу установки с цифровой подписью (версия 762 и выше), нажмите Yes:



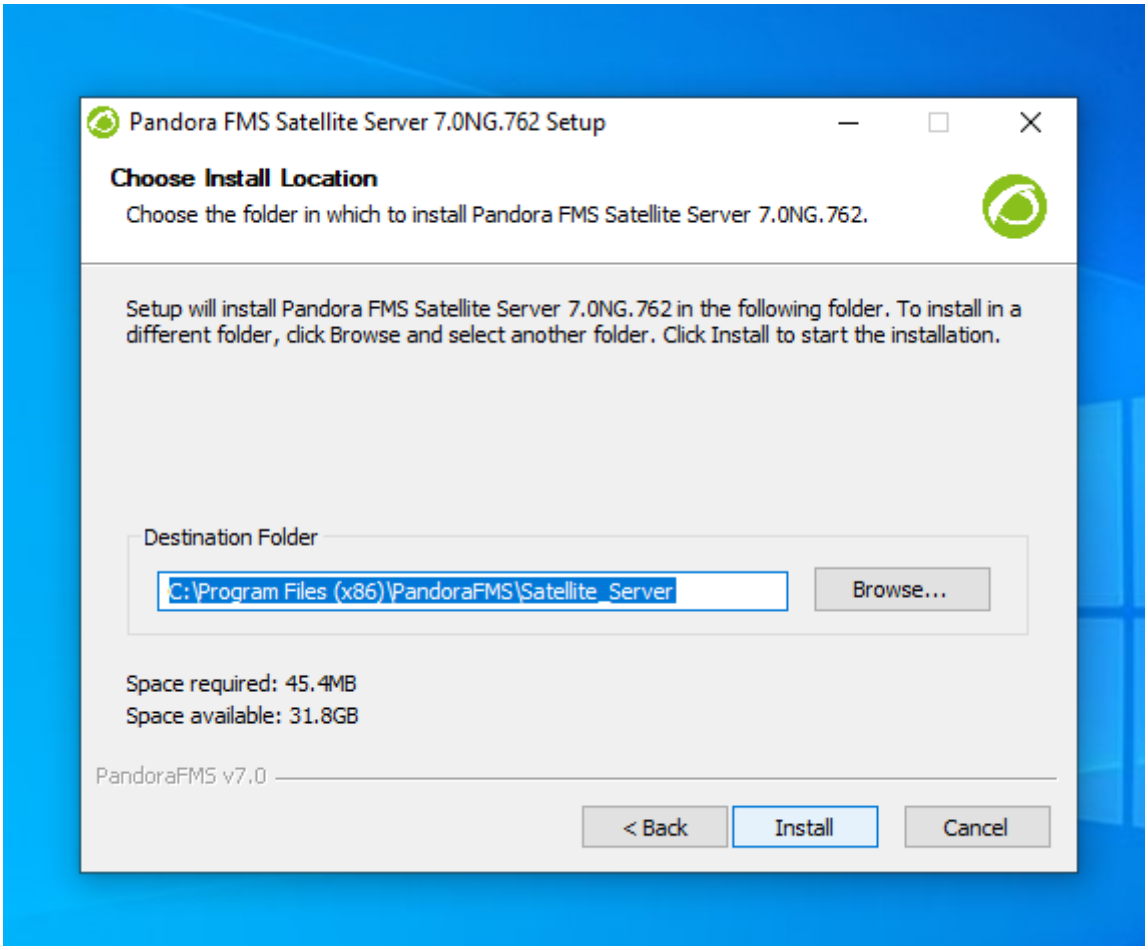
Выберите язык для установки:



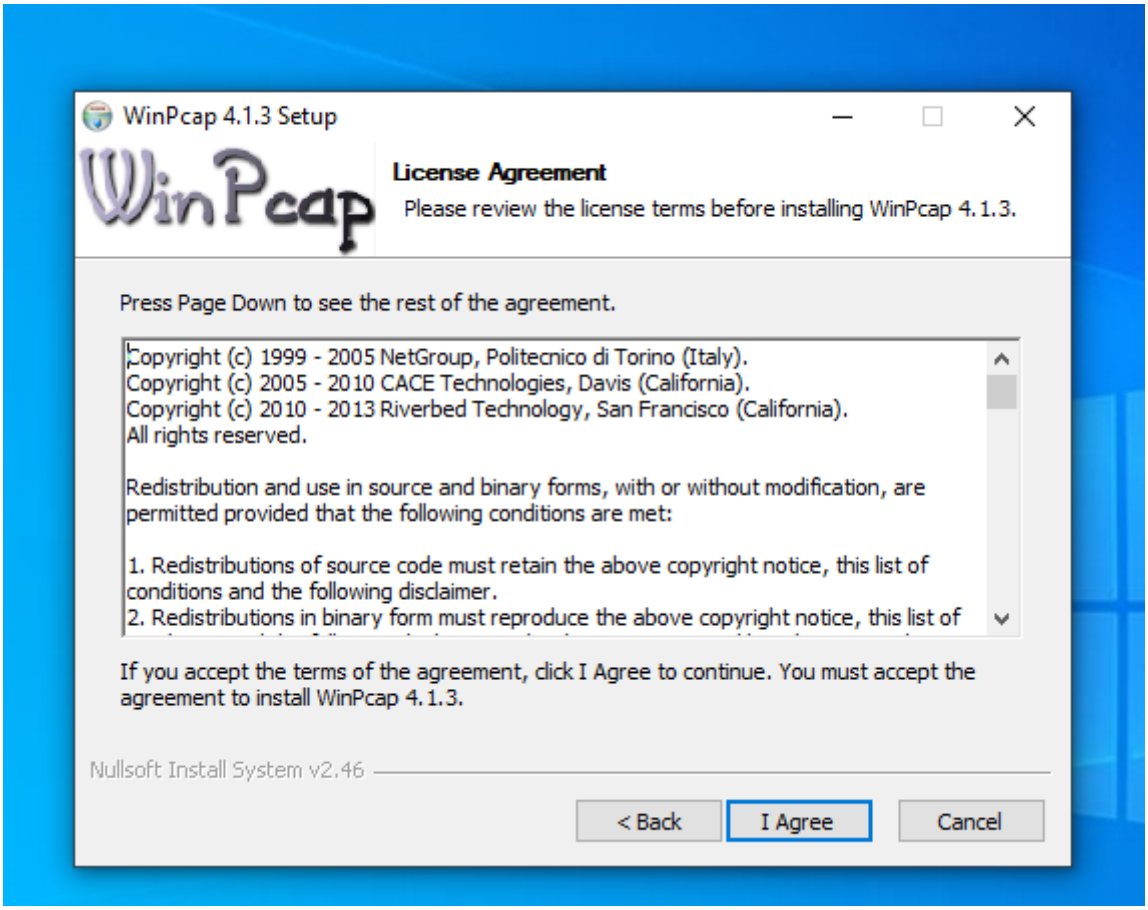
Нажмите на «Следующее»:



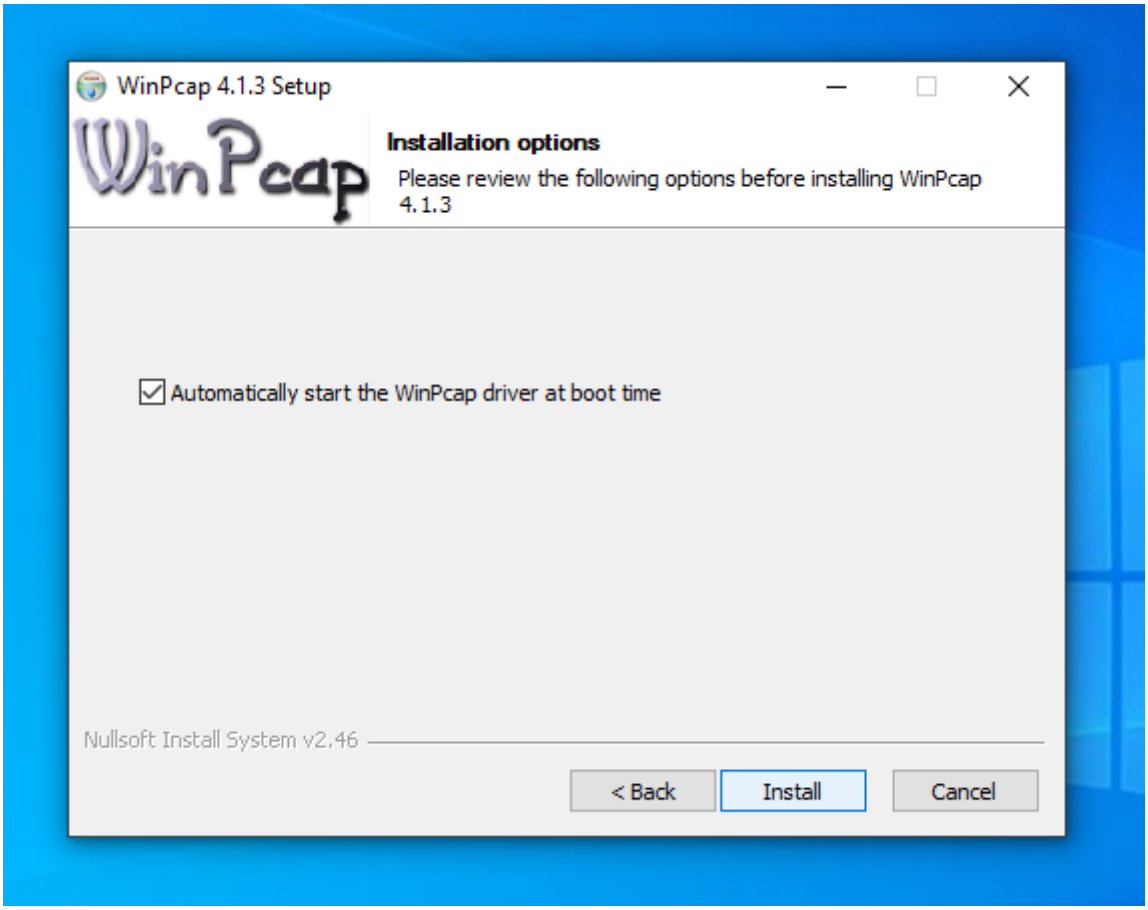
Выберите место для установки программы:



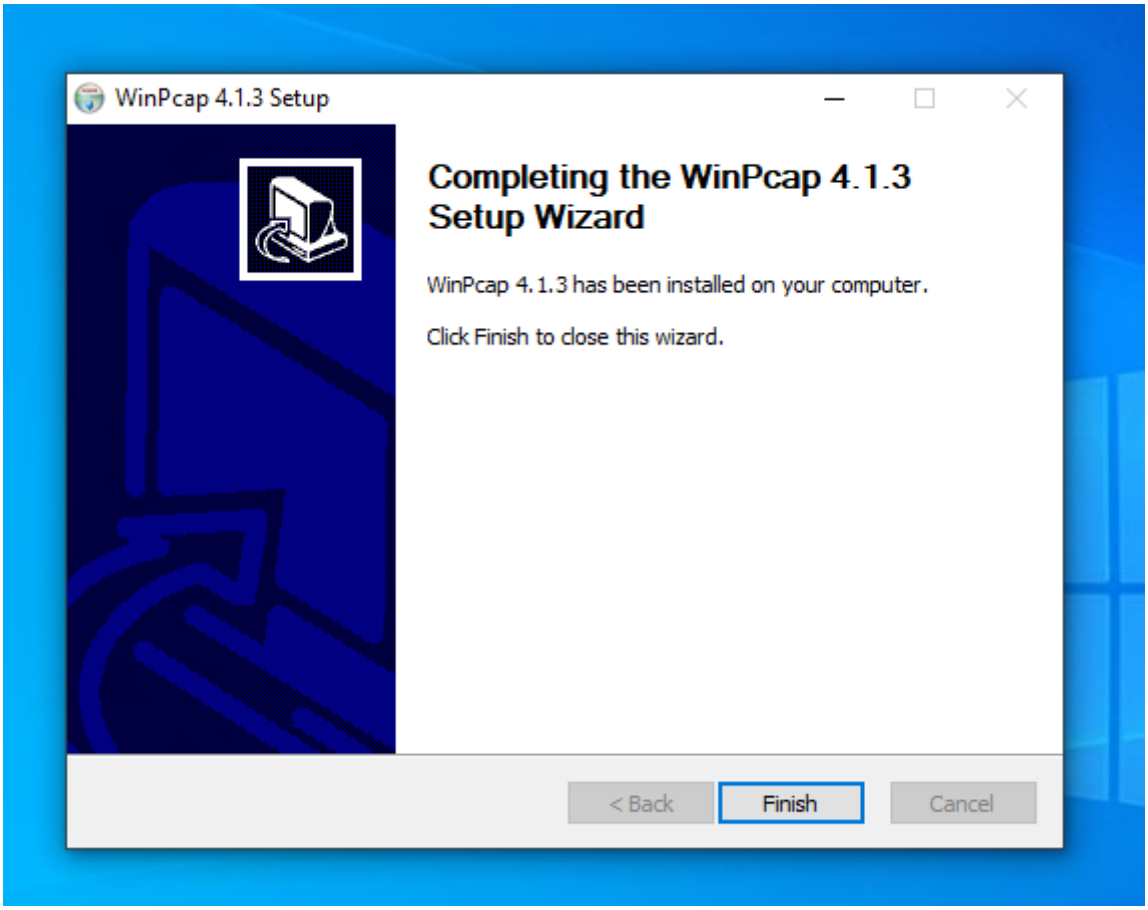
Также необходимо будет установить WinPCap. На этом этапе установки появится окно установки.



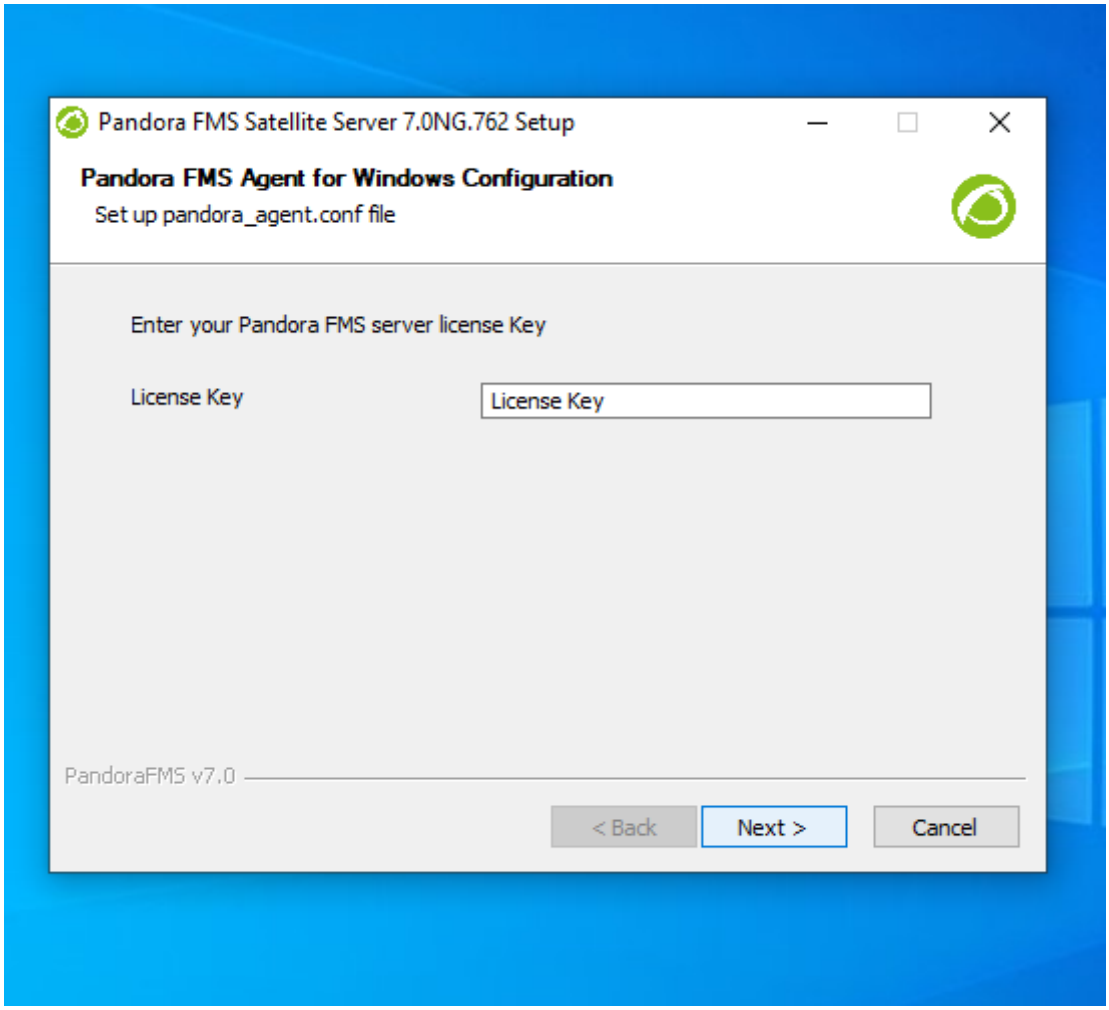
Установите включение WinPCap при запуске машины:



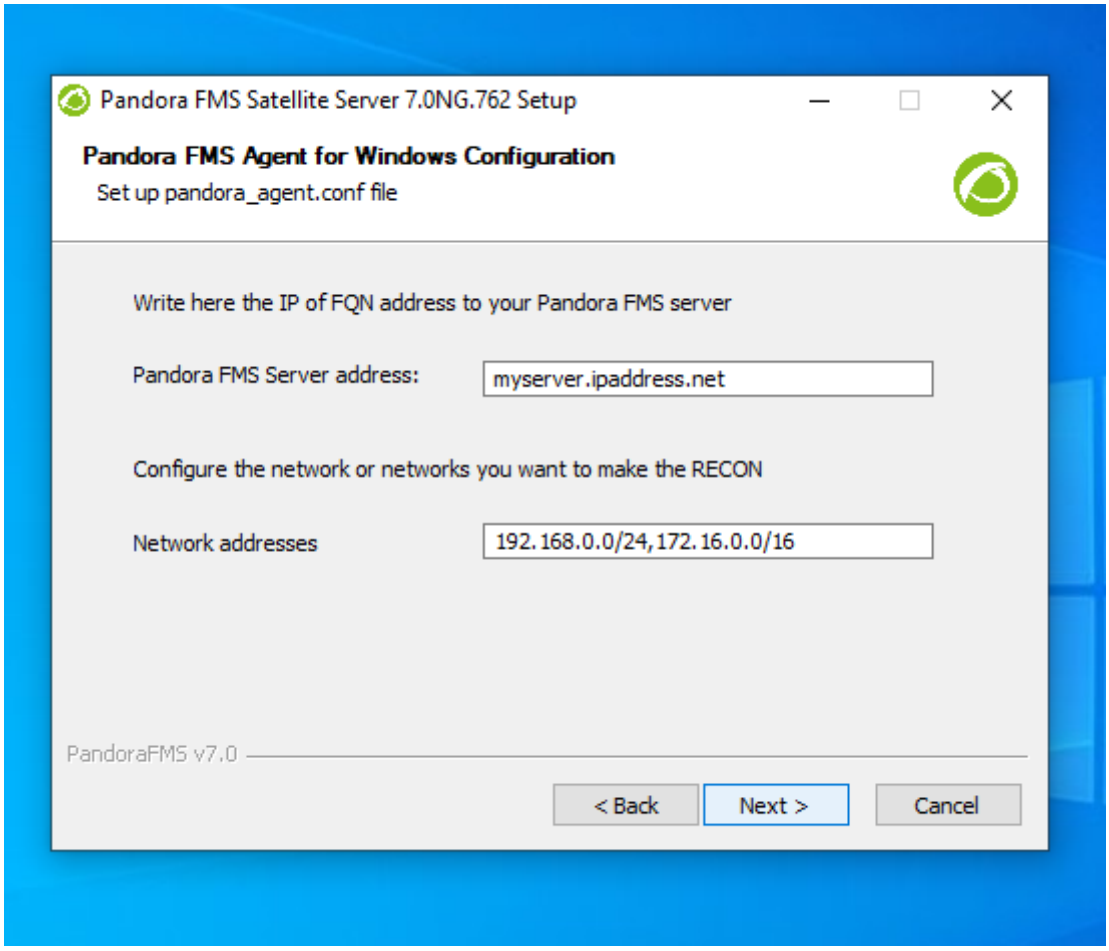
После завершения установки WinCap вы увидите следующий экран:



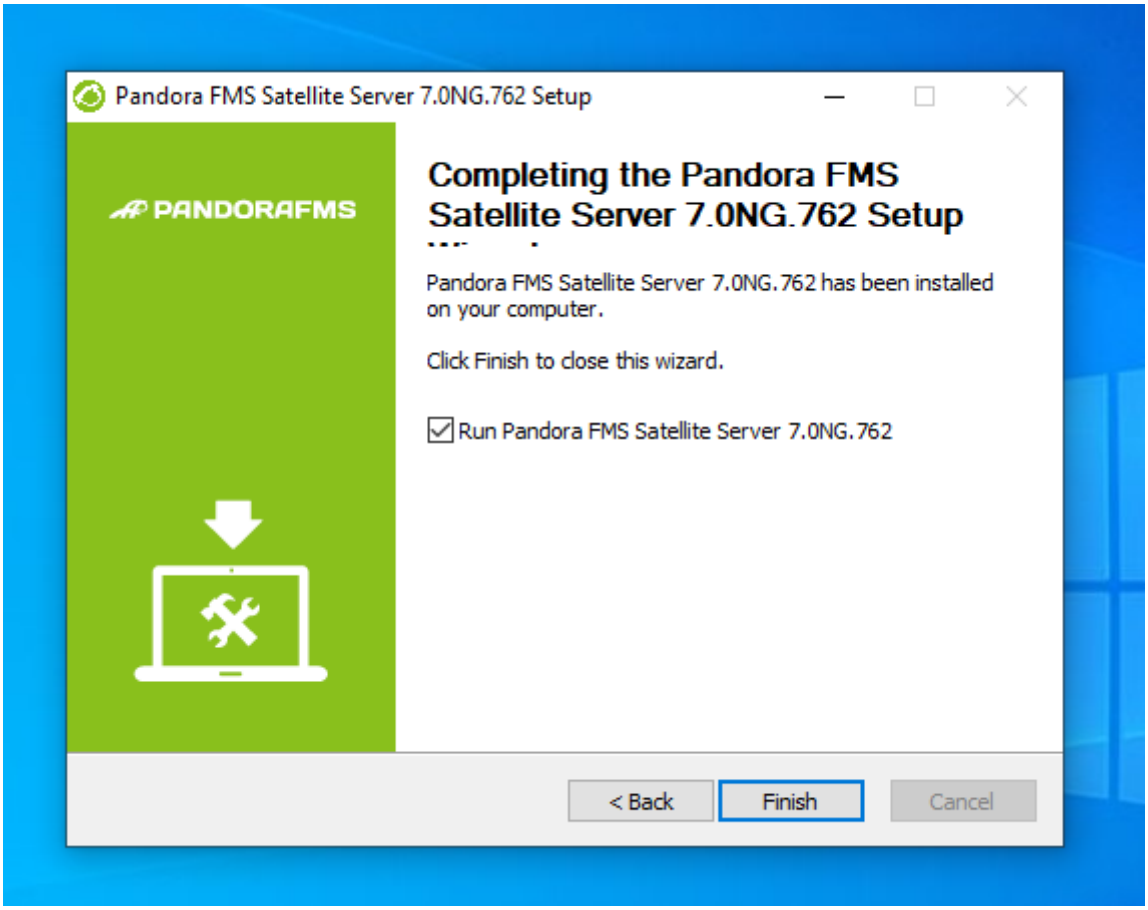
Введите лицензионный ключ Pandora FMS Enterprise, чтобы продолжить установку:



В следующем разделе необходимо настроить адрес сервера Pandora FMS для отправки данных; можно определить правила сканирования сети для Satellite Server.



Чтобы все изменения вступили в силу, необходимо перезагрузить машину.



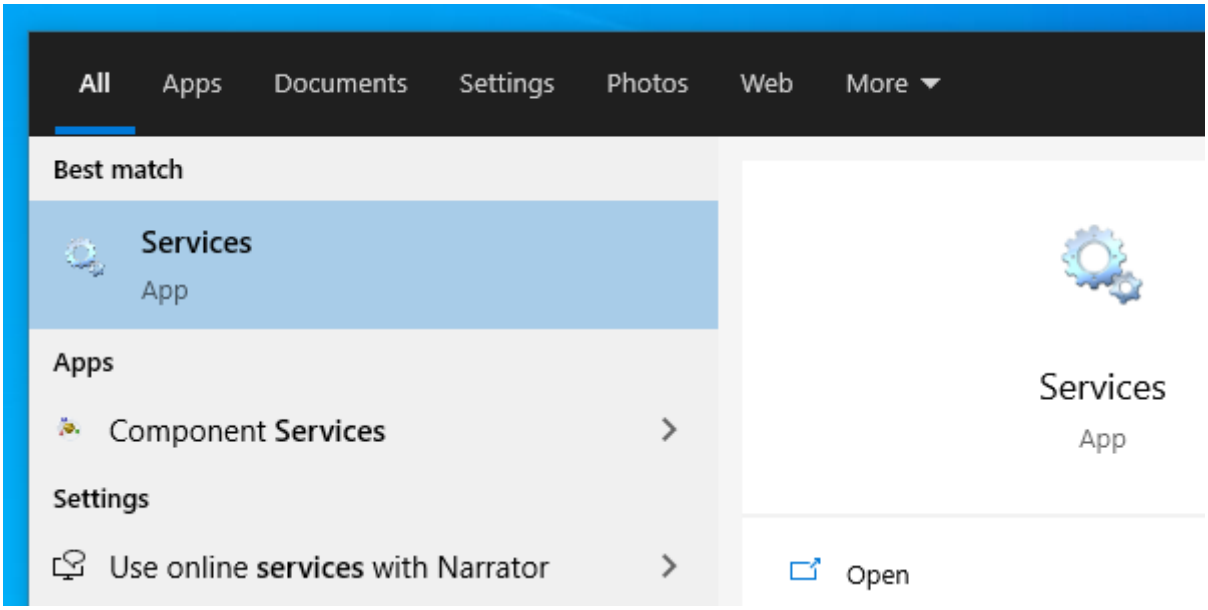
После завершения процесса вы можете запускать и останавливать службу Satellite Server PFMS из меню Пуск Windows.

Функционирование модулей WMI в некоторых версиях Windows

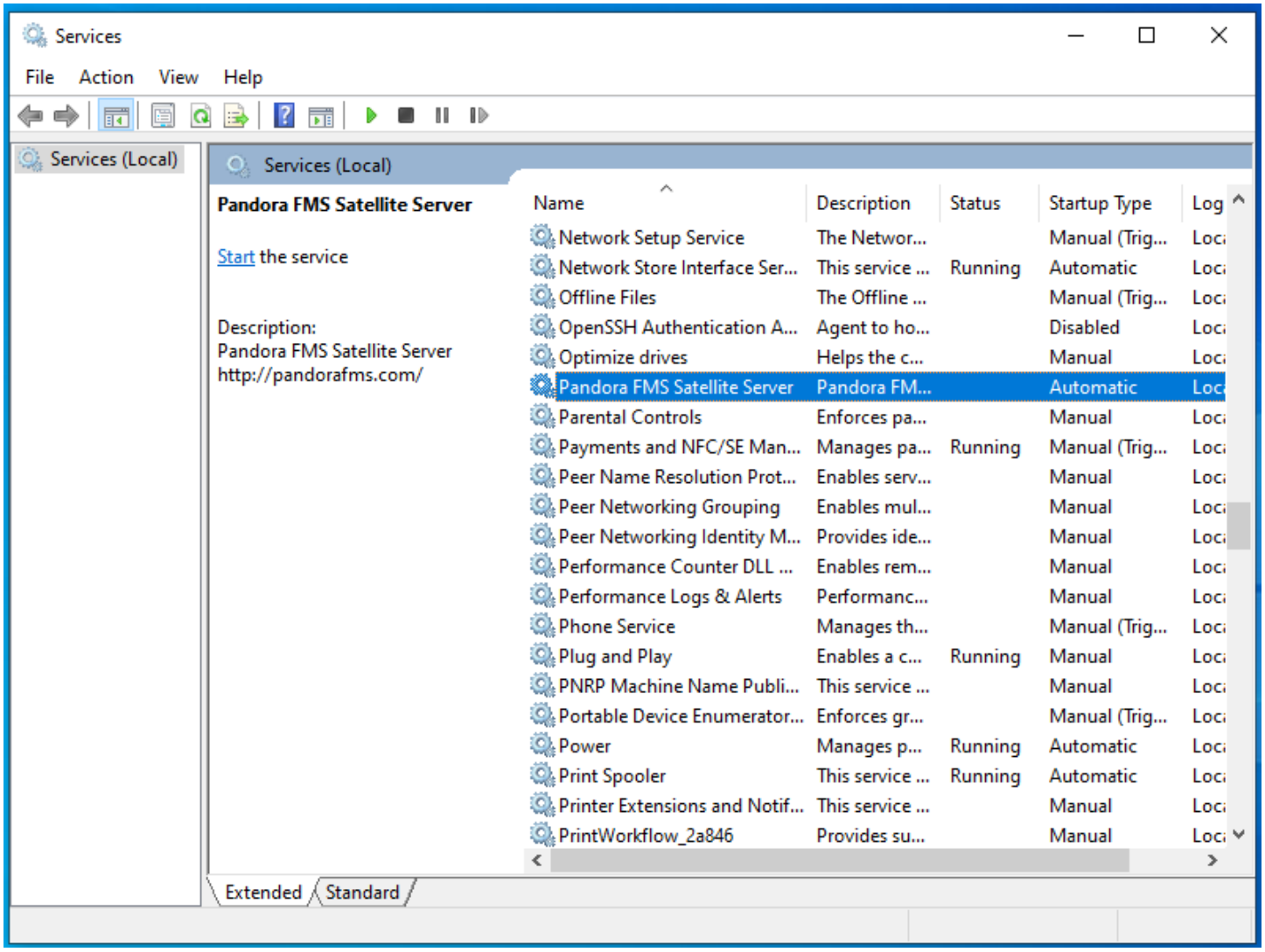
По соображениям безопасности Windows® в некоторых версиях ограничены пользователи для удаленных запросов WMI. В случае если эти запросы не могут осуществляться, решением является запуск службы Satellite Server от имени администратора.

Процесс должен происходить следующим образом:

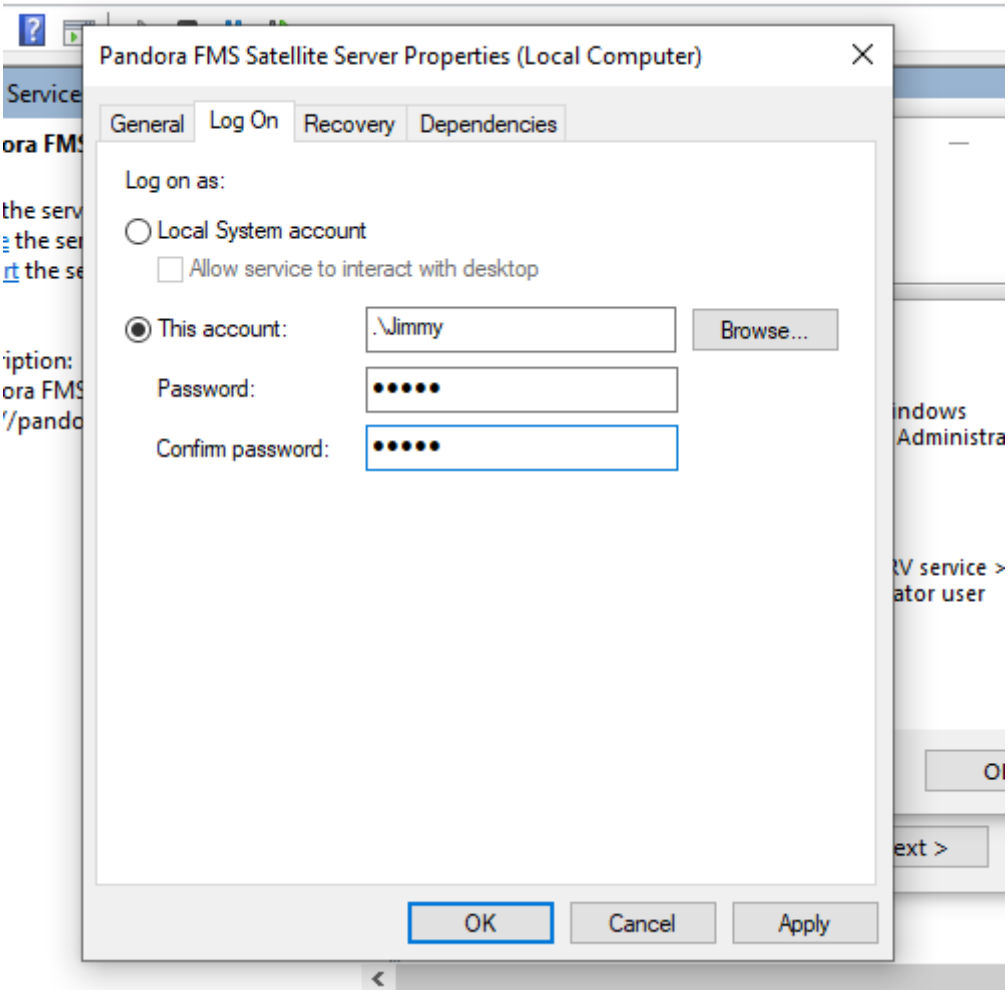
Откройте сервисы:



Нажмите на значок сервиса и зайдите в Свойства:



В окне Войти выберите учетную запись с правами администратора и примените изменения:



Для применения изменений необходимо перезапустить службу.

Настройка

Все параметры, требующие *тайм-аут* (время ожидания) должны быть указаны в секундах (по умолчанию 300 секунд равны 5 минутам).

Важно отметить, что время ответа и интервалы SNMP зависят от изменения состояния. В случае *булевых* проверок (состояние порта, состояние машины), порог, определяющий изменение состояния, является автоматическим. В случае числовых значений (задержка, сетевой трафик на интерфейсе, дисковое пространство, процессор и т.д.), он основывается на пороговом значении. По умолчанию пороговые значения не определяются; это необходимо сделать в определении модуля.

agent_interval

```
agent_interval xxx
```

По умолчанию, 300 секунд (5 минут). Это время, через которое данные отправляются на сервер, *независимо от того, делает ли проверки Satellite Server через более короткий*

интервал. При необходимости, а также по умолчанию, создайте Агентов на соответствующем сервере Pandora FMS в соответствии с указанным здесь временем.

agent_threads

```
agent_threads xxx
```

Количество потоков, используемых для отправки файлов данных XML.

xxxxxx_interval

```
xxxxxx_interval xxx
```

Выполняет все проверки (задержка, SNMP и т.д.) каждые xxx секунд. Если собранные данные отличаются от предыдущих, они будут отправлены в тот же момент. Если они не отличаются, то они будут отправлены, когда это прикажет интервал этого Агента. Полезно проводить очень интенсивные проверки и уведомлять только в случае изменения состояния.

xxxxx_retries

```
xxxxx_retries xxx
```

Количество повторов xxx при проверках (latency, SNMP, ping и т.д.).

xxxxx_timeout

```
xxxxx_timeout xxx
```

Таймаут в секундах для проверок типа SNMP, latency и ping.

xxxxx_block

```
xxxxx_block xxx
```

Заставляет сервер выполнять запросы (latency, ping и SNMP) блоками по XXX запросов. Чем выше это число (максимум 500), тем больше вы будете иметь вычислительной мощности, но это будет увеличивать задержки. В некоторых случаях целесообразно уменьшить это число.

xxxxx_threads

```
xxxxx_threads n
```

Количество потоков n, назначенных для каждого типа проверки для одновременной работы. Будут зависеть от мощности (процессора и оперативной памяти) машины. Чем больше потоков, тем больше нагрузка на систему, но тем большей вычислительной мощностью она будет обладать. При превышении 20 потоков, в зависимости от системы, производительность может ухудшиться.

log_file

```
log_file <path_file>
```

Указывает файл, в который записывается *журнал* Satellite Server, по умолчанию в `/var/log/satellite_server.log`.

recon_task

```
recon_task xxxxx[,yyyy]
```

IP-адреса/сети, используемые для автообнаружения, разделенные запятыми. Пример:

```
192.168.50.0/24,10.0.1.0/22,192.168.70.64/26
```

server_ip

```
server_ip <IP>
```

IP-адрес или DNS-имя сервера Pandora FMS для отправки информации. Данные будут отправлены через Tentacle, поэтому связь с сервером должна быть разрешена и защищена на порту `41121/tcp`.

recon_mode

```
recon_mode <mode_discovery>
```

Режим самообнаружения (`<mode_discovery>`) для использования. Система должна использовать следующие протоколы для обнаружения систем:

- `recon_mode icmp` Он проверяет, находится *ли хост* в сети (ping), и измеряет время задержки.
- `recon_mode snmp` Если устройство поддерживает SNMP (только v1 и v2), оно будет искать все

сетевые интерфейсы и получать трафик для всех из них, а также их рабочее состояние, имя и местоположение устройства. Он будет пытаться подключиться к различным сообществам, указанным в конфигурационном файле. *Для использования SNMP v3, распознавание которого не требуется* , перейдите по этой ссылке Как настроить известные учетные данные доступа.

- `recon_mode wmi` Аналогично предыдущему случаю, в данном случае показывается загрузка процессора, памяти и диска (все доступны).

recon_community

```
recon_community <aaa>,<bbb>,<ccc>...
```

Указывает список сообществ SNMP <xxx> для использования в обнаружении SNMP, разделенных запятыми. Используйте этот список при сканировании SNMP: для каждого найденного IP-адреса проверьте, отвечает ли он на одно из этих сообществ.

wmi_auth

```
wmi_auth Administrator%password[,user%pass]
```

Указывает список пар учетных данных пользователя, каждая из которых имеет формат <имя пользователя>%<пароль> и разделенные запятыми.

Например: `admin%1234,super%qwerty`. Использует этот список в сканировании WMI. Для каждого найденного IP-адреса проверьте, соответствует ли он какой-либо из этих комбинаций.

wmi_ntlmv2

```
wmi_ntlmv2 [0|1]
```

Активирует(1) или деактивирует (0) аутентификацию протокола NTLMv2 для WMI.

agent_conf_dir

```
agent_conf_dir <path>
```

Путь (<path>) к каталогу, в котором автоматически создаются и хранятся конфигурационные файлы каждого Агента, созданного Satellite Server. По умолчанию `/etc/pandora/conf`. Такие агенты также могут быть созданы вручную.

group

```
group <group_name>
```

Определите имя группы агентов `<group_name>` по умолчанию, созданных Satellite Server. Например, «Servers».

daemon

```
daemon [1|0]
```

Если его значение равно 1, он запускает *демона* (сервис) в фоновом режиме (значение по умолчанию).

hostfile

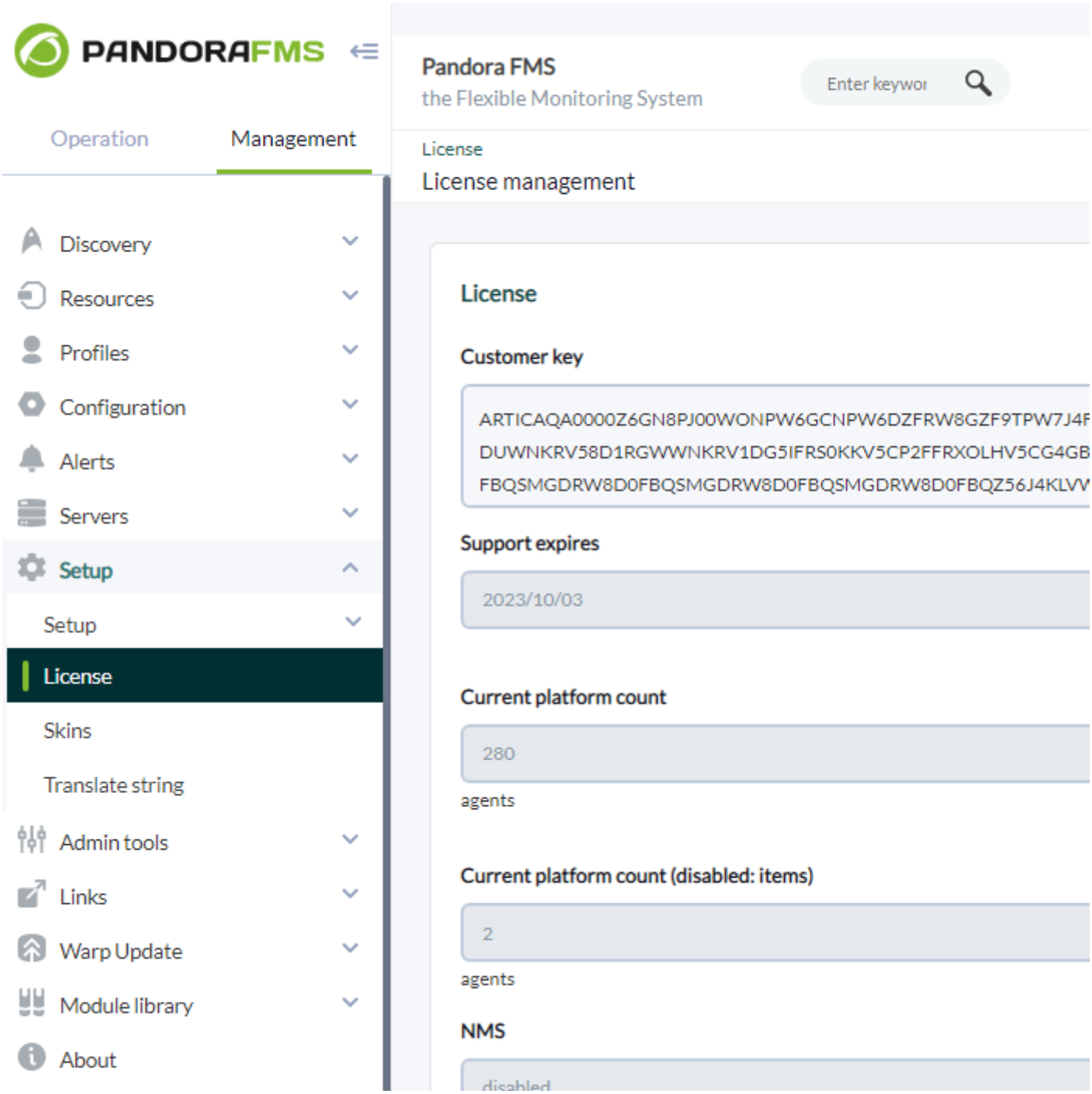
```
hostfile
```

Это альтернативный или дополнительный метод исследования сети для поиска *хостов*. В этом файле, каждая строка содержит один адрес. В качестве альтернативы, вы можете передать в той же строке имя хоста, за которым следует IP, тогда агент будет создан с этим именем и также будет использовать этот IP-адрес для модулей (например: `192.168.0.2 <hostname>`). При отправке запроса с Fping на определенные адреса, результат должен отображаться онлайн, чтобы эти адреса были действительными.

pandora_license

```
pandora_license xxxxxxx
```

Запишите и сохраните лицензию сервера Pandora FMS Enterprise, как показано в разделе Setup → License консоли Pandora FMS.



Вы можете использовать одну и ту же лицензию на стольких Satellite Servers, на скольких потребуется, поскольку общее количество Агентов, использующих лицензию, проверяется на сервере Pandora FMS, а не на Satellite Server.

remote_config

```
remote_config [1|0]
```

По умолчанию активирует удаленную конфигурацию для обнаруженных Агентов, необходимую, если вы хотите управлять ими из консоли после их обнаружения. Также позволяет удаленно конфигурировать сам Satellite Server.

temporal_min_size

```
temporal_min_size xxx
```

Если свободное пространство (в мегабайтах) ресурса, в котором находится временный каталог, меньше этого значения, пакеты данных не генерируются. Это предотвращает заполнение диска, если по какой-то причине соединение с сервером будет потеряно на длительный период времени.

xml_buffer

```
xml_buffer [0|1]
```

Значение по умолчанию 0. Если значение установлено на 1, агент сохранит XML-данные, которые ему не удалось отправить, чтобы повторить попытку позже.

На Unix, если вы находитесь в безопасной среде,
подумайте о смене временного каталога, поскольку
`/tmp` имеет права на запись для всех пользователей.

snmp_version

```
snmp_version xx
```

Версия SNMP, которая будет использоваться по умолчанию (1). Чтобы узнать, как пользоваться SNMP v3 перейдите по этой сслыке Как настроить известные учетные данные доступа.

При изменении этого значения некоторые модули
могут перестать работать.

braa

```
braa <path>
```

Путь `<path>` к двоичному файлу Braa. Значение по умолчанию `/usr/bin/braa`.

fping

```
fping <path>
```

Путь <path> к двоичному файлу Fping. Значение по умолчанию /usr/sbin/fping.

fsnmp

```
fsnmp <path>
```

Путь <path> к двоичному файлу Fsnmp. Значение по умолчанию /usr/bin/pandorafsnmp.

latency_packets

```
latency_packets xxx
```

Количество пакетов ICMP xxx, отправленных на запрос задержки.

nmap

```
nmap <path>
```

Путь <path> к двоичному файлу Nmap. Значение по умолчанию /usr/bin/nmap.

nmap_timing_template

```
nmap_timing_template x
```

Значение xxx, указывающее уровень агрессивности Nmap, от 1 до 5. Один означает медленнее, но надежнее, пять - быстрее, но менее надежно. Значение по умолчанию: 2.

ping_packets

```
ping_packets xxx
```

Количество ICMP-пакетов, отправленных за один ping.

recon_enabled

```
recon_enabled [0|1]
```

Активирует (1) или деактивирует (0) автообнаружение оборудования.

recon_timing_template

```
recon_timing_template xxx
```

Подобно nmap_timing_template, но применяется для сканирования сети.

server_port

```
server_port xxxxx
```

Порт сервера Tentacle.

server_name

```
server_name xxxxx
```

Имя сервера Satellite (по умолчанию принимает *hostname* машины).

server_path

```
server_path <path>
```

Путь <path>, по которому копируются файлы XML, если transfer_mode находится в локальной сети (по умолчанию `/var/spool/pandora/data_in`).

server_opts

Параметры сервера, которые передаются в Tentacle.

transfer_mode

```
transfer_mode [tentacle|local]
```

Режим передачи файлов. Это может быть только Тентакль или локальный (по умолчанию Тентакль).

Вторичный сервер

```
secondary_mode [on_error|always]
```

Особым типом общего параметра конфигурации является определение вторичного сервера. Он позволяет определить сервер, на который отправляются данные, в дополнение к стандартному серверу. Режим вторичного сервера работает двумя способами:

- on_error: Он будет отправлять данные на вторичный сервер только в том случае, если не может отправить их на первичный сервер.
- always: Данные всегда будут отправляться на вторичный сервер, независимо от того, можно ли связаться с первичным сервером или нет.

Пример конфигурации:

```
secondary_server_ip     192.168.1.123
secondary_server_path   /var/spool/pandora/data_in
secondary_mode          on_error
secondary_transfer_mode tentacle
secondary_server_port   41121
```

snmp_verify

```
snmp_verify [0|1]
```

Включает (1) или выключает (0) проверку модулей SNMP v1, которые вызывают сбой Braa в реальном времени. Эти модули будут отброшены и больше не будут выполняться. Смотрите как snmp2_verify, так и snmp3_verify.

snmp2_verify

```
snmp2_verify [0|1]
```

Включает (1) или выключает (0) проверку модулей SNMP v2, которые вызывают сбой Braa в реальном времени. Эти модули будут отброшены и больше не будут выполняться. Смотрите как snmp_verify, как и snmp3_verify.

Проверка модулей SNMP версии 2 может быть очень медленной!

snmp3_verify

```
snmp3_verify [0|1]
```

Включает (1) или выключает (0) проверку модулей SNMPv3, которые вызывают сбой Braa в

режиме реального времени. Эти модули будут отброшены и больше не будут выполняться. Смотрите как snmp_verify, так и snmp2_verify.

startup_delay

```
startup_delay xxx
```

Подождите xxx секунд перед первой отправкой файлов данных.

temporal

```
temporal <directory>
```

Временный каталог, в котором создаются файлы XML, по умолчанию `/tmp`.

tentacle_client

```
tentacle_client <path>
```

Путь <path> клиента Tentacle. Значение по умолчанию `/usr/bin/tentacle_client`.

wmi_client

```
wmi_client <path>
```

Путь <path> к двоичному файлу wmi_client. Значение по умолчанию `/usr/bin/wmic`.

snmp_blacklist

```
snmp_blacklist <path>
```

Путь <path> к списку выполнения модулей SNMP. Значение по умолчанию `/etc/pandora/satellite_server.blacklist`.

add_host

```
add_host <IP-адреса> [имя_агента]
```

Добавляет указанный *хост* в список отслеживаемых агентов. После IP-адреса можно указать имя агента. Можно добавить несколько *хостов*, по одному в каждой отдельной строке.

Например:

```
add_host 192.168.0.1
add_host 192.168.0.2 localhost.localdomain
```

ignore_host

```
ignore_host <agent_name>
```

Удаляет указанный *хост* из списка контролируемых Агентов, даже если он обнаружен при выполнении задачи сканирования сети Recon Task. *Хост* должен быть идентифицирован именем Агента. Можно игнорировать несколько *хостов*, по одному на строку. Например:

```
ignore_host 192.168.0.1
ignore_host localhost.localdomain
```

keepalive

```
keepalive xxx
```

Satellite Server сообщает о своем состоянии и проверяет изменения в удаленной конфигурации (Агентов и своей) каждые xxx секунд. Значение по умолчанию: 30 секунд.

credential_pass

```
credential_pass xxx
```

Пароль, используемый для *шифрования паролей полей учетных записей*. Он должен совпадать с тем, который определен в консоли Pandora FMS. По умолчанию используется имя *хоста*.

timeout_bin

```
timeout_bin <path>
```

Если определено, то программа timeout (обычно `/usr/bin/timeout`) будет использоваться при вызове клиента Tentacle.

timeout_seconds

```
timeout_seconds xxx
```

Время ожидания, в секундах, для программы тайм-аут. Параметр timeout_bin должен быть настроен.

proxy_traps_to

```
proxy_traps_to <dir_IP[:port]>
```

Перенаправляет SNMP-ловушки, полученные Спутниковым сервером, на указанный адрес (и порт, опционально). По умолчанию используется порт 162.

proxy_tentacle_from

```
proxy_tentacle_from <dir_IP[:port]>
```

Перенаправляет данные, полученные Tentacle Server с указанного адреса (и порта, опционально). По умолчанию используется порт 41121.

proxy_tentacle_to

```
proxy_tentacle_to <dir_IP[:port]>
```

Перенаправляет запросы клиентов Tentacle, полученные Satellite Server, на указанный адрес (и порт, опционально). По умолчанию используется порт 41121.

Эта опция может конфликтовать с удаленной конфигурацией агентов, если вы собираетесь использовать Satellite Server в качестве *прокси* для некоторых программных агентов и контролировать их удаленно с самого Satellite Server (ICMP, SNMP и т.д.) с включенной удаленной конфигурацией в обоих случаях. В этой ситуации вам следует либо использовать разные Агенты для проводимых проверок (т.е. с разными `agent_name`), либо оставить удаленную конфигурацию включенной только в одном из них (Satellite Server или Software Agents).

dynamic_inc

```
dynamic_inc [0|1]
```

При значении 1 он перемещает автоматически обнаруженные динамические модули (SNMP, WMI...) в отдельные файлы, чтобы они не мешали удаленной настройке Агентов.

vlan_cache_enabled

```
vlan_cache_enabled [0|1]
```

Активирует(1) или деактивирует (0) *кэш* VLAN автообнаруженных *хостов*.

verbosity

```
verbosity <0-10>
```

Уровень детализации в записи *лога*, где 10 - самый подробный уровень информации.

agents_blacklist_icmp

Версия NG 713 или выше.

```
agents_blacklist_icmp 10.0.0.0/24[,8.8.8.8/30]
```

Список исключений для проверок ICMP. Это поле может быть сконфигурировано со списком IP-адресов с использованием примечания CIDR для предотвращения выполнения дальнейших модулей типа ICMP. Можно указать несколько подсетей, разделяя их запятыми.

agents_blacklist_snmp

Версия NG 713 или выше.

```
agents_blacklist_snmp 10.0.0.0/24[,8.8.8.8/30] (Version> 7.0OUM713)
```

Список исключений для проверок SNMP. Это поле может быть сконфигурировано со списком IP-адресов с использованием примечания CIDR для предотвращения работы большего количества модулей типа SNMP. Можно указать несколько подсетей, разделяя их запятыми.

agents_blacklist_wmi

Версия NG 713 или выше.

```
agents_blacklist_wmi 10.0.0.0/24[,8.8.8.8/30]
```

Список исключений для проверок WMI. Это поле может быть сконфигурировано со списком IP-адресов с использованием примечания CIDR для предотвращения дальнейшего запуска модулей WMI. Можно указать несколько подсетей, разделяя их запятыми.

general_gis_exec

Версия NG 734 или выше.

```
general_gis_exec xxx
```

При включении этой опции будет использоваться *скрипт* для обеспечения GIS-позиционирования для всех Агентов, обнаруженных Спутниковым сервером. *Скрипт* должен быть разрешен для запуска и печати координат в формате <долгота>,<широта>,[<высота>] Третий параметр, высота, является необязательным.

forced_add

Если установлено значение 1, хосты, добавленные вручную (через host_file или add_host), всегда будут создаваться, даже если они не отвечают на ping, с конфигурационным файлом без модулей.

Создание агентов в Satellite Server

Существует три способа создания агентов на спутниковом сервере: Recon Task, файл satellite_hosts.txt или вручную создавая .conf агентов для мониторинга.

Создание агентов через Recon Task

Создание агентов с помощью Recon Task является наиболее часто используемым среди пользователей Pandora FMS. Для этого мы должны получить доступ к файлу конфигурации Satellite Server и настроить следующие параметры:

- recon_community: Необходимо указать разделенный запятыми список сообществ SNMP для использования при обнаружении SNMP (в случае выполнения задачи Recon типа SNMP).
- recon_enabled: Должно быть установлено значение 1, чтобы включить задачу Recon спутникового сервера.
- recon_interval: Интервал времени, в течение которого сканируется сеть, в секундах (по умолчанию 604800 секунд, 7 дней).
- recon_mode: Режим выполнения Recon Task (SNMP,ICMP,WMI), разделенные запятыми.

- recon_task: Список сетей, которые необходимо исследовать, разделенных запятыми.
- recon_timing_template: Значение, указывающее, насколько агрессивным должен быть nmap, от 1 до 5. Один означает медленнее, но надежнее; пять означает быстрее, но менее надежно (по умолчанию 3).

Пример выполнения Recon Task:

```
recon_community public
recon_enabled 1
recon_interval 604800
recon_mode icmp,snmp,wmi
recon_task 192.168.0.0/24,192.168.1.0/24
recon_timing_template 3
```

После того как данные настроены, запустите Спутниковый сервер с помощью команды:

```
/etc/init.d/satellite_serverd start
```

Агенты, конфигурационные файлы которых не содержат никаких модулей, игнорируются Спутниковым сервером.

Создание агентов с помощью файла

Прежде всего, чтобы создать агента через файл satellite_hosts.txt, необходимо зайти в файл конфигурации Satellite Server и удалить строку комментария:

```
host_file /etc/pandora/satellite_hosts.txt
```

Во-вторых, необходимо создать файл по ранее указанному пути с IP-адресами *хостов*, которые вы хотите создать, поместив IP-адрес и имя создаваемого Агента:

```
192.168.10.5 Server5
192.168.10.6 Server6
192.168.10.7 Server7
```

РДля того чтобы Агенты с этими IP-адресами были созданы, они должны ответить на вызов fping, иначе они не будут созданы.

После того как данные настроены, запускаем Satellite Server с помощью команды:

```
/etc/init.d/satellite_serverd start
```

Указанный файл читается каждые recon_interval секунд(ы).

Создание агентов вручную

В каталоге `/etc/pandora/conf` (по умолчанию) размещаются конфигурационные файлы новых Агентов. Откройте терминал продажи и перейдите в эту папку:

```
cd /etc/pandora/conf
```

Создайте файл с расширением `.conf`, например «file.conf». Заполните следующие поля вручную:

- agent_name: Имя, которое будет присвоено агенту.
- agent_alias: Псевдонимы, которые будут присвоены агенту.
- address: IP-адрес элемента, подлежащего мониторингу.
- group: Группа, в которую нужно назначить агента.
- gis_exec: *Скрипт* позиционирования (необязательно). Если используется, он перезаписывает местоположение, указанное параметром general_gis_exec Спутникового сервера.
- Добавьте модули, которые будут созданы в агенте.

Примером может быть:

```
agent_name Example
agent_alias This is an example
address 127.0.0.1
group Servers

module_begin
module_name Ping
module_ping
module_end

module_begin
module_name Latency
module_latency
module_end
```

После того как данные настроены, запустите Satellite Server с помощью команды:

```
/etc/init.d/satellite_serverd start
```

Удаление агентов в Satellite Server

Вы можете выполнить полное удаление Агентов или частичное удаление Агентов.

Прежде чем приступить к работе, создайте резервную
копию всех папок и файлов в них.

Для полного удаления Агентов мы должны принять во внимание метод, использованный при создании Агентов:

- Manual: Прежде всего, необходимо удалить файлы `.conf` агентов, созданные в папке `/etc/pandora/conf`, а затем удалить агентов в консоли.
- Файл satellite_hosts.txt: Вам придется удалить этот файл, а также `.conf`, созданный в папке `/etc/pandora/conf`, а затем удалить агентов в консоли.
- Recon_task: Необходимо будет отключить конфигурацию `recon_task` в файле `.conf` Спутникового сервера, удалить `.conf`, которые создались в папке `/etc/pandora/conf` и после этого удалить агенты из консоли.

Для частичного удаления мы также должны учитывать метод, использованный при создании Агентов.

- Manual: Сначала необходимо удалить файлы `.conf` удаляемых Агентов в папке `/etc/pandora/conf`, а затем удалить Агенты в консоли.
- Файл Satellite_hosts.txt: Вам придется удалить из файла строки IP-адресов, которые нужно удалить, а также `.conf`, которые были созданы в папке `/etc/pandora/conf` с этими IP-адресами, а затем удалить Агенты в консоли.
- Recon_task: Вам придется настроить список исключений `recon_task` в файле `.conf` Спутникового сервера, затем удалить `.conf`, созданный в папке `/etc/pandora/conf` с этими IP-адресами, и удалить Агентов в консоли.

Индивидуальные конфигурации для каждого агента

В дополнение к «автоматическим» модулям, любые доступные проверки TCP, SNMP, WMI или SSH могут быть добавлены к мониторингу, используя синтаксис, аналогичный тому, который используется для локальных модулей в Программных агентах. Приведены некоторые примеры допустимых модулей для Satellite Server, самостоятельно сгенерированных после обнаружения системы.

¡Убедитесь, что OID начинаются с точки, иначе модули
SNMP не будут работать!

Состояние интерфейса через SNMP. Спутниковый сервер автоматически обнаруживает каждый интерфейс:

```
 module_begin
 module_name if eth1 OperStatus
 module_description IP address N/A. Description: The current operational state
of the interface. The testing(3) state indicates that no operational packets can
```

```
be passed.
 module_type generic_data_string
 module_snmp 192.168.70.225
 module_oid .1.3.6.1.2.1.2.2.1.8.3
 module_community artica06
 module_end
```

Чтобы заставить модуль использовать SNMP версии 2c, добавьте строку:

```
module_version 2c
```

Чтобы заставить модуль использовать SNMP версии 1, добавьте строку:

```
module_version 1
```

Например:

```
 module_begin
 module_name if eth1 OperStatus
 module_description IP address N/A. Description: The current operational state
of the interface. The testing(3) state indicates that no operational packets can
be passed.
 module_type generic_data_string
 module_snmp 192.168.70.225
 module_version 2c
 module_oid .1.3.6.1.2.1.2.2.1.8.3
 module_community artica06
 module_end
```

Подключение к машине (через PING):

```
 module_begin
 module_name ping
 module_type generic_data
 module_ping 192.168.70.225
 module_end
```

Проверка порта (через TCP):

```
 module_begin
 module_name Port 80
 module_type generic_proc
 module_tcp
 module_port 80
 module_end
```

Общий запрос SNMP. В этом случае Спутниковый сервер автоматически извлекает трафик из каждого интерфейса с его описательным «реальным» именем:

```
 module_begin
 module_name if eth0 OutOctets
 module_description The total number of octets transmitted out of the interface,
including framing characters.
 module_type generic_data_inc
 module_snmp 192.168.70.225
 module_oid .1.3.6.1.2.1.2.2.1.16.2
 module_community public
 module_end
```

WMI-запрос на использование ЦП (в процентах):

```
 module_begin
 module_name CPU
 module_type generic_data
 module_wmicpu 192.168.30.3
 module_wmiauth admin%none
 module_end
```

WMI-запрос свободной памяти (в процентах):

```
 module_begin
 module_name FreeMemory
 module_type generic_data
 module_wmimem 192.168.30.3
 module_wmiauth admin%none
 module_end
```

Общий запрос WMI:

```
 module_begin
 module_name GenericWMI
 module_type generic_data_string
 module_wmi 192.168.30.3
 module_wmiquery SELECT Name FROM Win32_ComputerSystem
 module_wmiauth admin%none
 module_end
```

Общая команда SSH:

```
 module_begin
 module_name GenericSSH
 module_type generic_data
 module_ssh 192.168.30.3
 module_command ls /tmp | wc -l
 module_end
```

Чтобы ввести порог, это необходимо сделать как в текстовом определении модуля (`module_min_warning`, `module_min_critical`), так и при определении порогов через веб-

интерфейс. Например:

```
module_begin
module_name Latency
module_type generic_data
module_latency 192.168.70.225
module_min_warning 80
module_min_critical 120
module_end
```

Вы можете вручную создавать модули выполнения. *Скрипты* или команды, выполняемые Satellite Server, должны быть предварительно развернуты и доступны для Satellite Server. В этом смысле он работает так же, как `module_exec` Агента. Обратите внимание, что использование `module_exec` может привести к снижению производительности Satellite Server.

```
module_begin
module_name Sample_Remote_Exec
module_type generic_data
module_exec /usr/share/test/test.sh 192.168.50.20
module_min_warning 90
module_min_critical 95
module_end
```

Начиная с 7-й версии Pandora FMS, можно добавлять *плагины*. Следует отметить, что *плагины* запускаются на машине, на которой запущен Satellite Server. Поэтому необходимо будет реализовать в этих *плагинах* способ подключения к удаленному оборудованию, которое необходимо контролировать. Преимущество этого метода перед предыдущими заключается в его большей гибкости. Таким образом, вы можете реализовать условия и другие механизмы, для которых `module_exec` не подходит. Синтаксис такой же, как и для Агентов. Примером использования *плагина* может быть следующее:

```
module_plugin /usr/share/pandora/remote_advanced_checks.sh 192.168.0.1
```

SNMPv3

Чтобы настроить модуль SNMPv3, установитеmodule_version на 3 и определите:

- `module_seclevel`: Уровень безопасности (`noauth`, `authnopriv` или `authpriv`).
- `module_secname`: Имя безопасности.
- `module_authproto`: Протокол аутентификации (`md5` или `sha`).
- `module_authpass`: Ключ аутентификации.
- `module_privproto`: Протокол конфиденциальности (`aes` или `des`).
- `module_privpass`: Ключ конфиденциальности, при необходимости.

Например:

```
module_begin
module_name snmp_noauth
module_type generic_data_string
module_snmp 127.0.0.1
module_version 3
module_oid .1.3.6.1.2.1.1.1.0
module_seclevel noauth
module_secname snmpuser
module_end
```

```
module_begin
module_name snmp_authnopriv
module_type generic_data_string
module_snmp 127.0.0.1
module_version 3
module_oid .1.3.6.1.2.1.1.2.0
module_seclevel authnopriv
module_secname snmpuser
module_authproto md5
module_authpass 12345678
module_end
```

```
module_begin
module_name snmp_authpriv
module_type generic_data_string
module_snmp 127.0.0.1
module_version 3
module_oid .1.3.6.1.2.1.1.2.0
module_seclevel authpriv
module_secname snmpuser
module_authproto sha
module_authpass 12345678
module_privproto aes
module_privpass 12345678
module_end
```

Конкретная конфигурация SNMPv3 может быть разделена между модулями путем изъятия ее из описания модуля, в случае если она одинакова для всех (она также может быть разделена между агентами путем перемещения ее в файл конфигурации сервера-спутника):

```
agent_name snmp
address 127.0.0.1

seclevel authpriv
secname snmpuser
authproto md5
authpass 12345678
privproto des
privpass 12345678
```

```
module_begin
module_name snmp_authpriv_1
module_type generic_data_string
module_snmp
module_version 3
module_oid .1.3.6.1.2.1.1.1.0
module_end

module_begin
module_name snmp_authpriv_2
module_type generic_data_string
module_snmp
module_version 3
module_oid .1.3.6.1.2.1.1.2.0
module_end
```

Поля для учетных даных

Если аутентификация не настроена с использованием закрытого и открытого ключей, для работы модулей SSH требуется имя пользователя (<user>) и пароль (<pass>). Оба регистрируются в главном конфигурационном файле `satellite_server.conf` с помощью поля для учетных даных (`credential_box`) в следующих форматах:

red/маска, пользователь, пароль

red/маска, пользователь,[[зашифрованный пароль|]]

Например:

```
credential_box 192.168.1.1/32,<user>,<pass1>
credential_box 192.168.1.0/24,<user>,<pass2>
```

Поиск в полях учетных данных осуществляется от более к менее строгим.

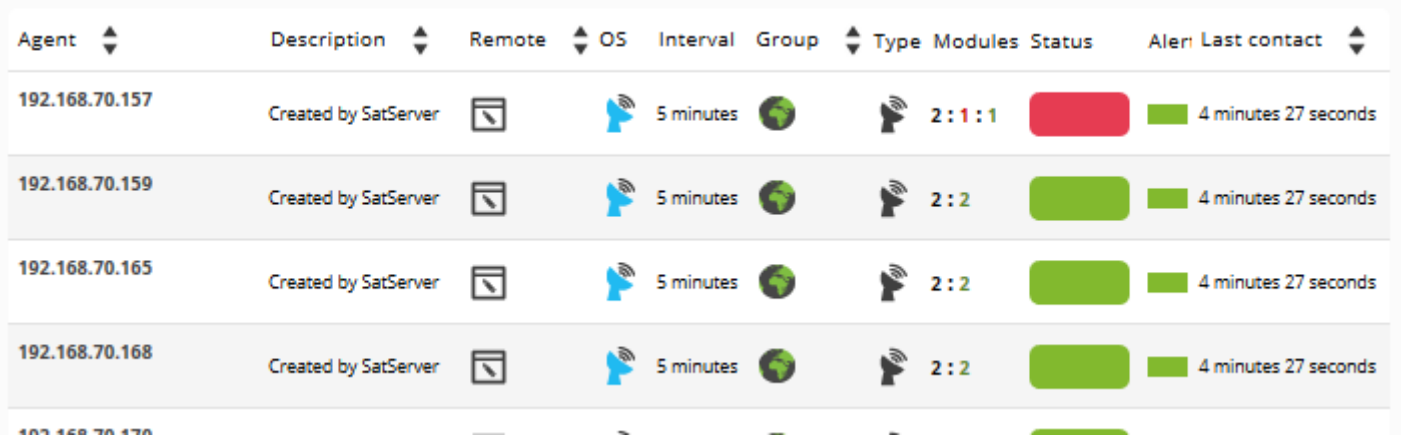
Пароли можно зашифровать с помощью Blowfish в режиме ECB. Убедитесь, что credential_pass определено, иначе *имя хоста* будет использоваться в качестве пароля шифрования по умолчанию. Шестнадцатеричное представление шифрованного текста должно быть окружено двойными квадратными скобками:

```
credential_box 192.168.1.0/24,<user>,[[80b51b60786b3de2|]]
```

Консольный просмотр всех агентов

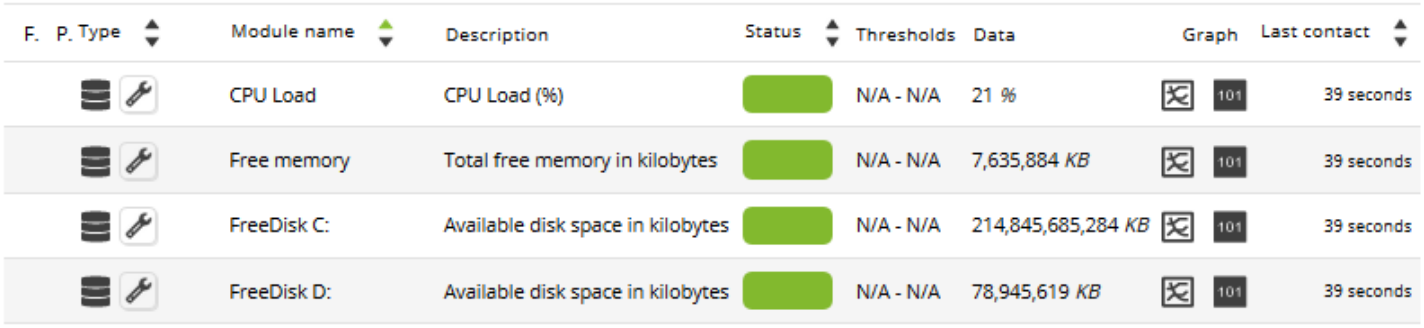
Если Спутниковый сервер настроен правильно, вы должны получить представление агента,

которое выглядит следующим образом:



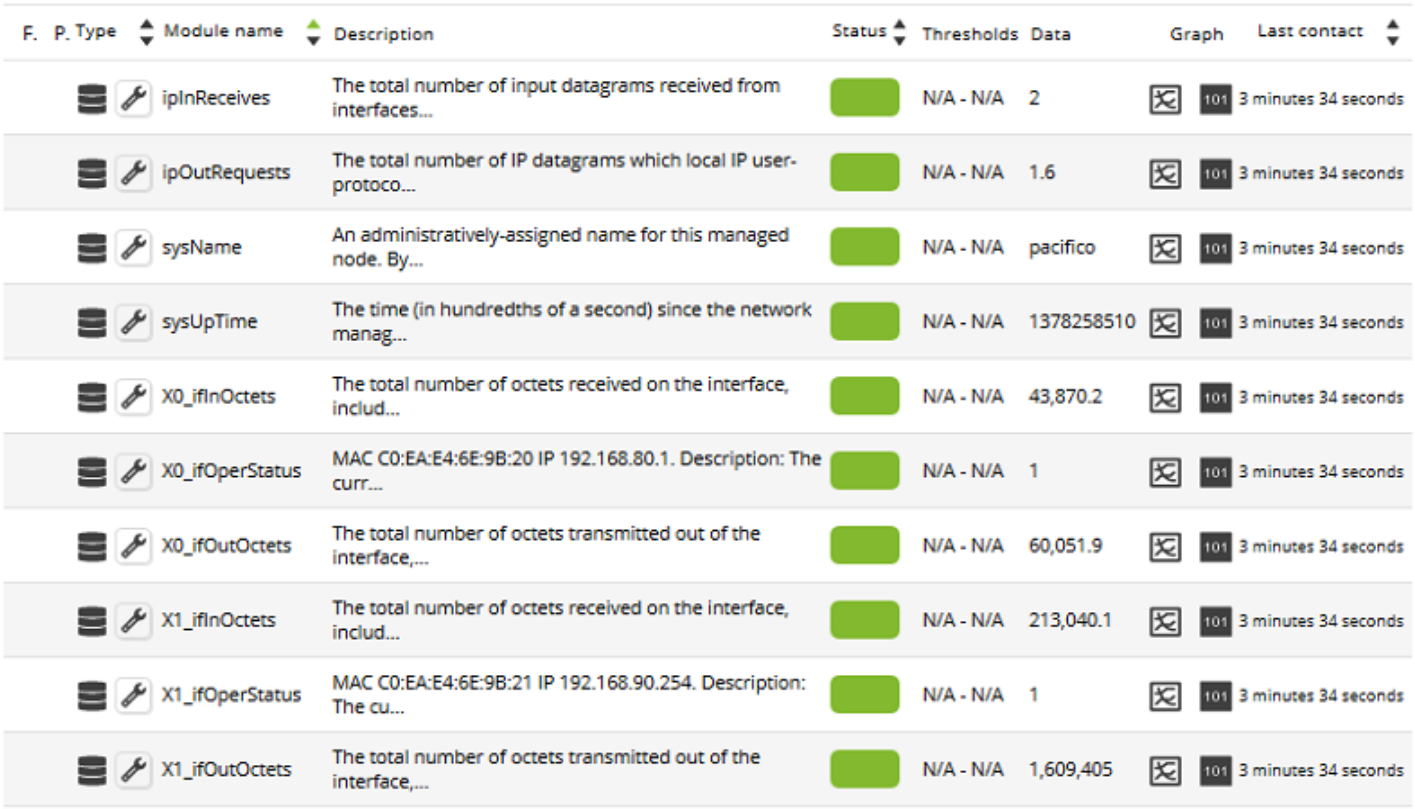
Agent	Description	Remote	OS	Interval	Group	Type	Modules	Status	Alert	Last contact
192.168.70.157	Created by SatServer			5 minutes			2 : 1 : 1			4 minutes 27 seconds
192.168.70.159	Created by SatServer			5 minutes			2 : 2			4 minutes 27 seconds
192.168.70.165	Created by SatServer			5 minutes			2 : 2			4 minutes 27 seconds
192.168.70.168	Created by SatServer			5 minutes			2 : 2			4 minutes 27 seconds

Как правило, модули ICMP (Ping и Latency) создаются на всех машинах, но некоторые могут также генерировать модули SNMP и WMI. Для тех, у кого включен WMI, будут созданы следующие модули, если они доступны:



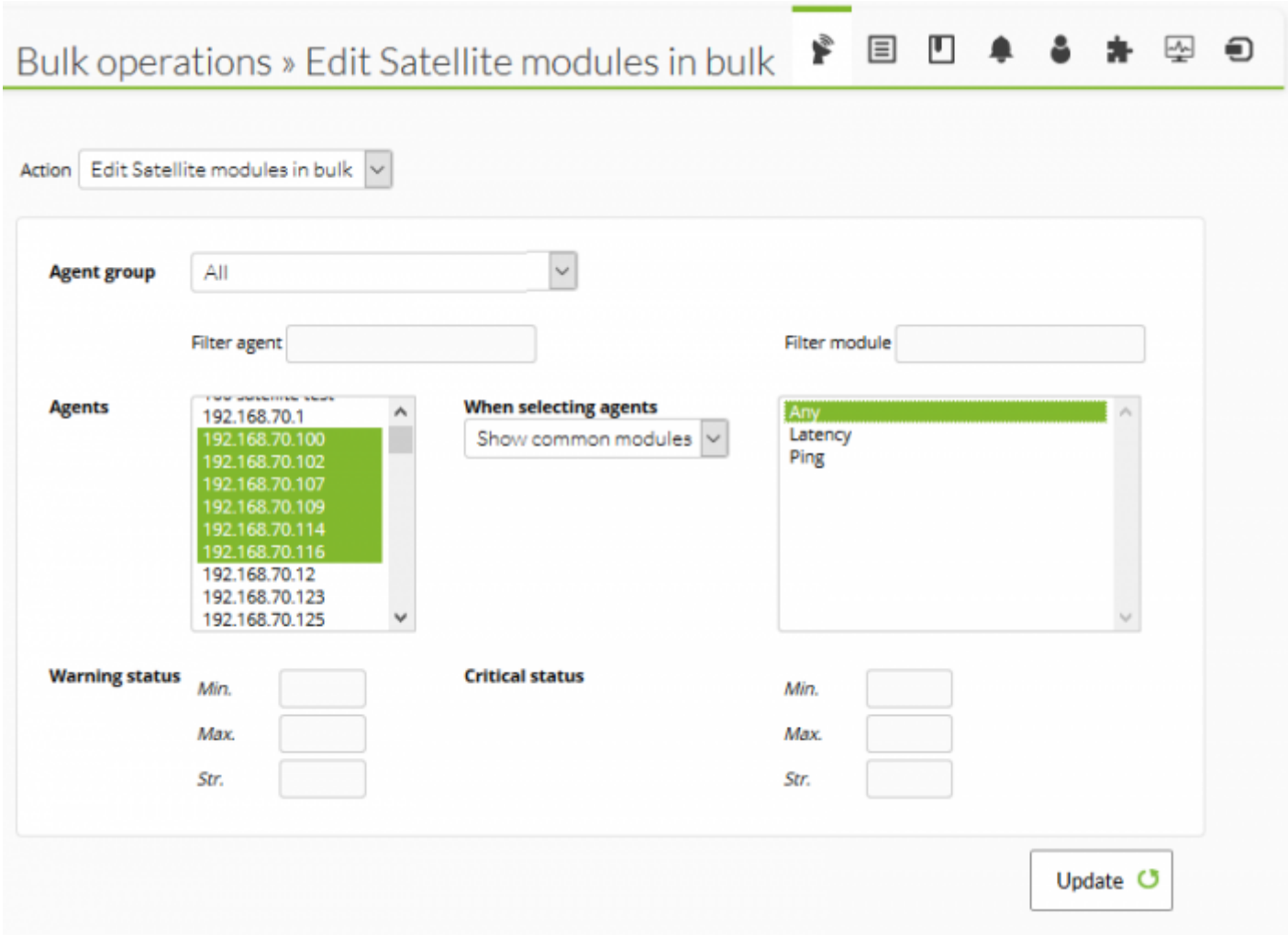
F.	P.	Type	Module name	Description	Status	Thresholds	Data	Graph	Last contact
			CPU Load	CPU Load (%)		N/A - N/A	21 %		39 seconds
			Free memory	Total free memory in kilobytes		N/A - N/A	7,635,884 *KB*		39 seconds
			FreeDisk C:	Available disk space in kilobytes		N/A - N/A	214,845,685,284 *KB*		39 seconds
			FreeDisk D:	Available disk space in kilobytes		N/A - N/A	78,945,619 *KB*		39 seconds

На машинах с поддержкой SNMP будут созданы следующие модули, если они доступны:



F.	P.	Type	Module name	Description	Status	Thresholds	Data	Graph	Last contact
			ipInReceives	The total number of input datagrams received from interfaces...		N/A - N/A	2		3 minutes 34 seconds
			ipOutRequests	The total number of IP datagrams which local IP user-protoco...		N/A - N/A	1.6		3 minutes 34 seconds
			sysName	An administratively-assigned name for this managed node. By...		N/A - N/A	pacifico		3 minutes 34 seconds
			sysUpTime	The time (in hundredths of a second) since the network manag...		N/A - N/A	1378258510		3 minutes 34 seconds
			X0_ifInOctets	The total number of octets received on the interface, includ...		N/A - N/A	43,870.2		3 minutes 34 seconds
			X0_ifOperStatus	MAC C0:EA:E4:6E:9B:20 IP 192.168.80.1. Description: The curr...		N/A - N/A	1		3 minutes 34 seconds
			X0_ifOutOctets	The total number of octets transmitted out of the interface,...		N/A - N/A	60,051.9		3 minutes 34 seconds
			X1_ifInOctets	The total number of octets received on the interface, includ...		N/A - N/A	213,040.1		3 minutes 34 seconds
			X1_ifOperStatus	MAC C0:EA:E4:6E:9B:21 IP 192.168.90.254. Description: The cu...		N/A - N/A	1		3 minutes 34 seconds
			X1_ifOutOctets	The total number of octets transmitted out of the interface,...		N/A - N/A	1,609,405		3 minutes 34 seconds

В разделе массовых операций консоли Pandora FMS есть специальный раздел, посвященный спутниковому серверу, где вы можете выполнить несколько действий для массового редактирования и удаления Агентов и Модулей.:



Список исключений SNMP

При мониторинге больших сетей модули SNMP, возвращающие недостоверные данные, могут повлиять на производительность Спутникового сервера и перевести другие модули в состояние «Неизвестно». Чтобы избежать этого, Satellite Server может считывать *список исключений* модулей SNMP, которые будут отбрасываться при запуске перед выполнением.

Чтобы создать список исключений, отредактируйте файл конфигурации `/etc/pandora/satellite_server.conf` и убедитесь в том, что `snmp_blacklist` является *не откомментированным* и настроен на путь к файлу, где будут храниться модули списка исключений. Далее выполните:

```
satellite_server -v /etc/pandora/satellite_server.conf
```

Перезапустите Satellite Server. Список исключений может быть регенерирован столько раз, сколько необходимо.

Формат списка исключений:

```
agent:OID
agent:OID
...
```

Например:

```
192.168.0.1:.1.3.6.1.4.1.9.9.27
192.168.0.2:.1.3.6.1.4.1.9.9.27
```

Вернуться в оглавление Документации Pandora FMS