Discovery

Discovery

Вернуться в оглавление Pandora FMS

Что такое Pandora FMS Discovery?

Версия NG 732 или выше.

Discovery предоставляет набор инструментов для упрощения мониторинга с помощью мастеров. Более подробную информацию вы можете получить в обучающем видео «Обучение Pandora FMS Discovery»

Task list

Инструмент Pandora FMS Discovery позволяет увидеть список всех запланированных задач в нашей среде как на уровне консоли, так и на уровне сервера.

Discovery Applications

Позволяет контролировать среды MySQL®, Oracle® или VMware® с новой консоли управления.

Discovery Cloud

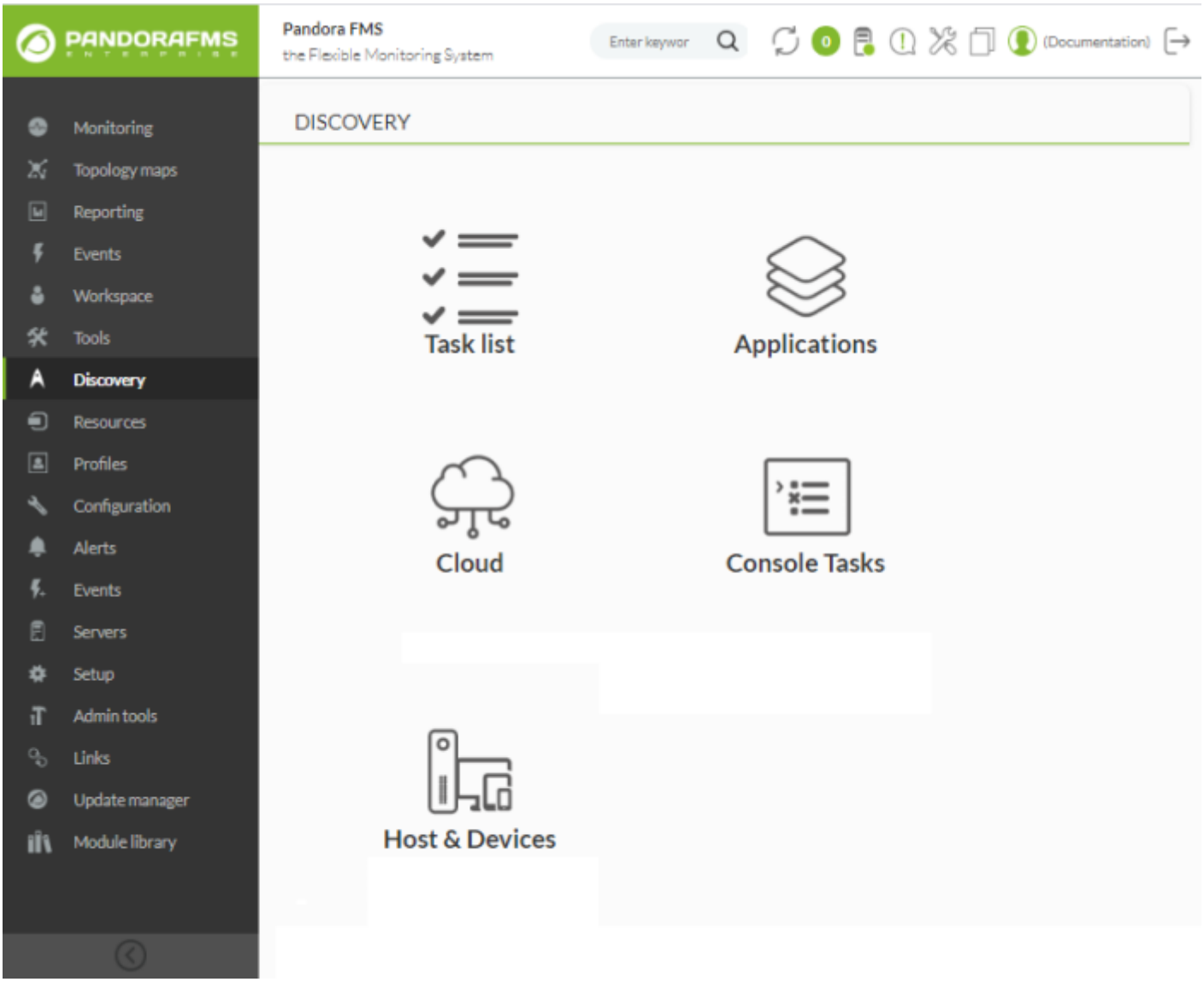
С помощью этой утилиты вы можете контролировать свою облачную инфраструктуру, от виртуальных машин, созданных в Amazon Web Services® (EC2) или реляционных баз данных в AWS RDS®, до виртуальных машин, работающих в Azure Computer®.

Console Tasks

Позволяет автоматизировать задачи консоли внутри системы Discovery, а также планировать отчеты, создавать резервные копии данных или выполнять пользовательские сценарии из консоли Pandora FMS.

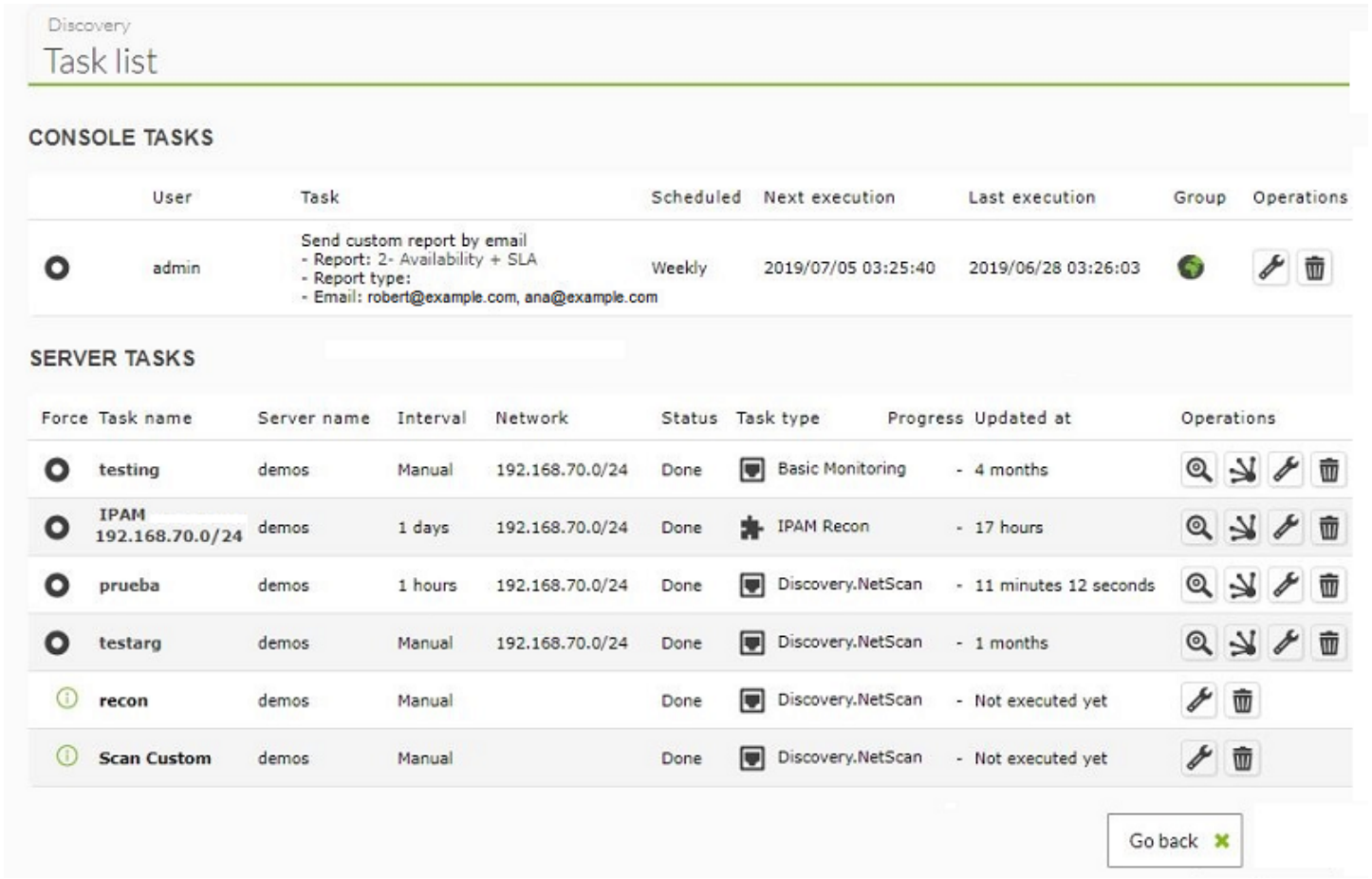
Discovery Host&Devices

Включает инструменты, необходимые для обнаружения или импорта устройств и компьютеров в сети.

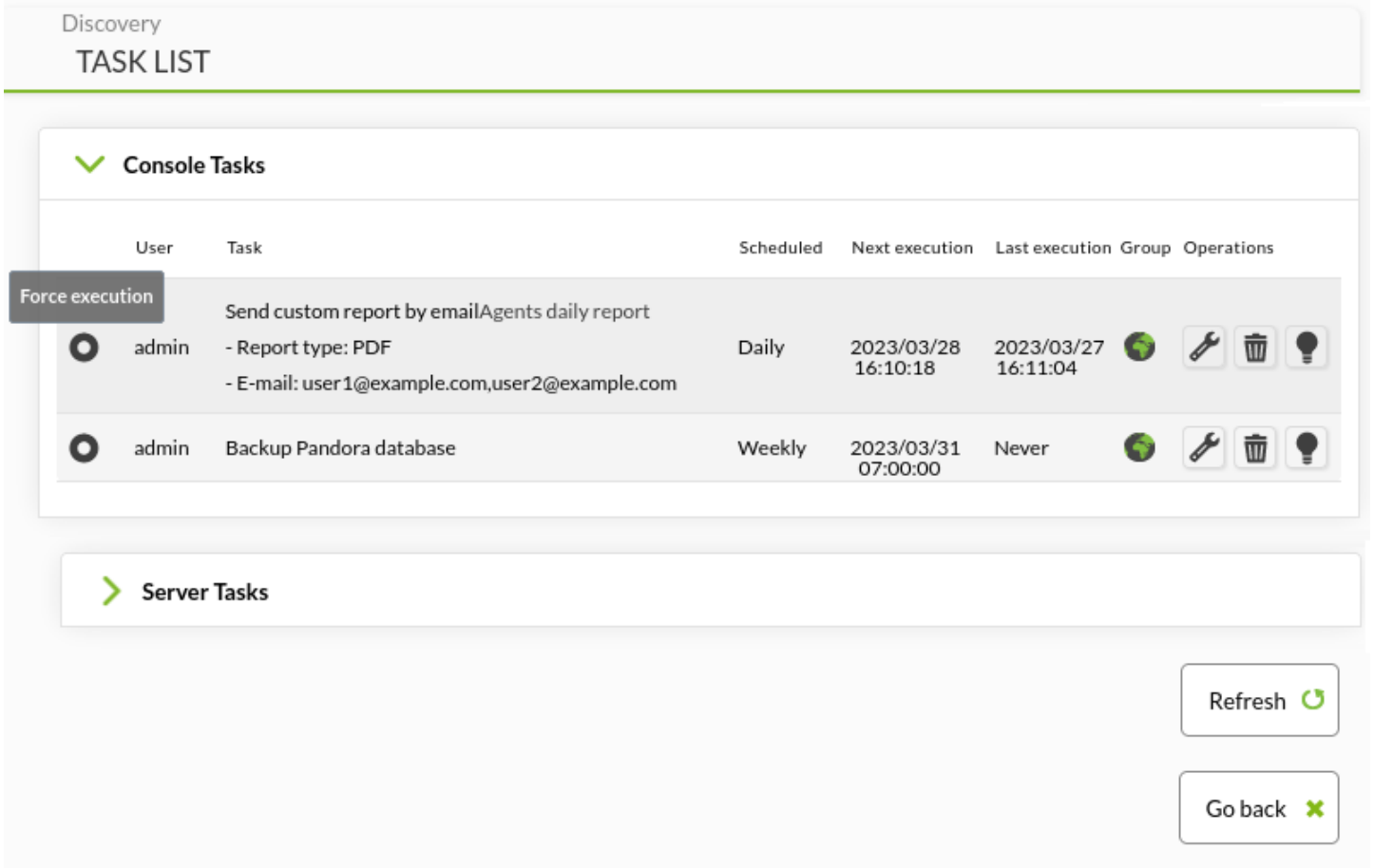


Discovery Task list

Инструмент Pandora FMS Discovery позволяет увидеть список всех задач, запрограммированных в среде, как на уровне консоли Console Tasks так и на уровне сервера Server Tasks.



Console tasks

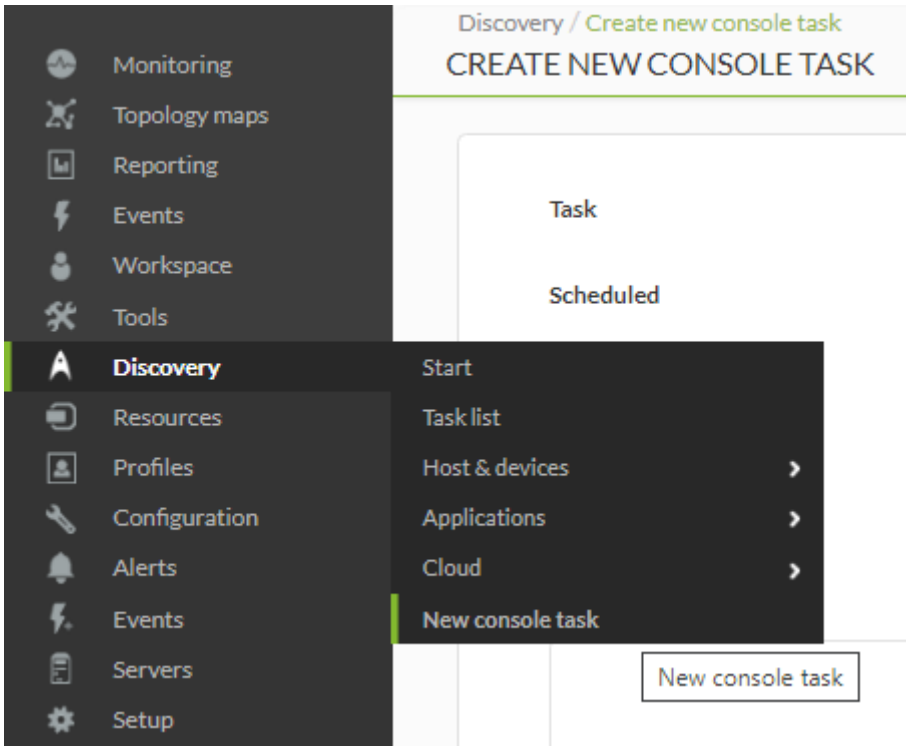


Для каждой из перечисленных задач (Console task):

- User: Тот, кто создает задачу.
- Task: краткая информация.
- Scheduled: Планирование по календарю.
- Next Execution: Указывает следующее выполнение.
- Last Execution: Указывает на время последнего выполнения задачи.
- Group: Группа, к которой она принадлежит.
- Operations: Отображает действия, которые могут быть выполнены для текущего пользователя; в данном примере их два - редактирование и удаление .

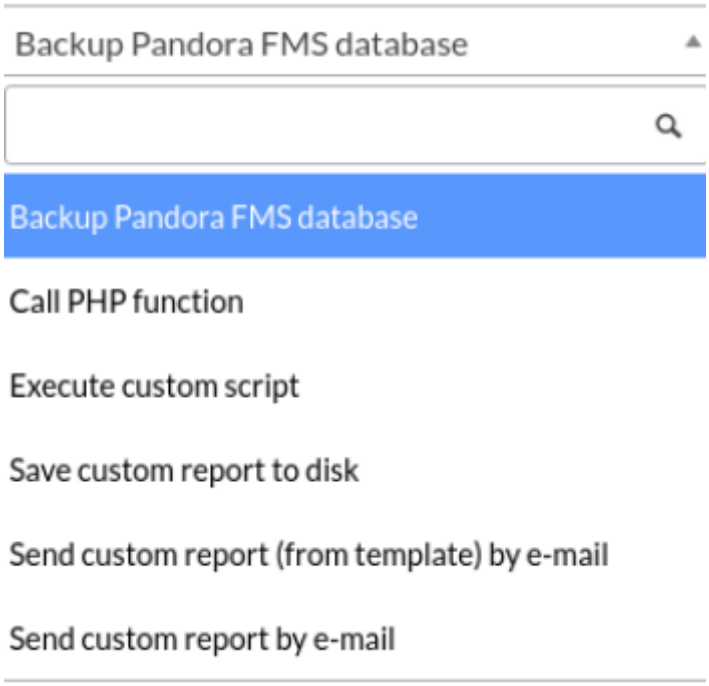
Создание или редактирование задач консоли

Чтобы *создать* консольную задачу, перейдите в Discovery → New console task.



Для *редактирования* задачи Console нажмите на значок , описанный в предыдущем разделе.

В обоих случаях интерфейс одинаков, за исключением соответствующей кнопки для создания (Create) или редактирования (Update) и сохранения изменений.

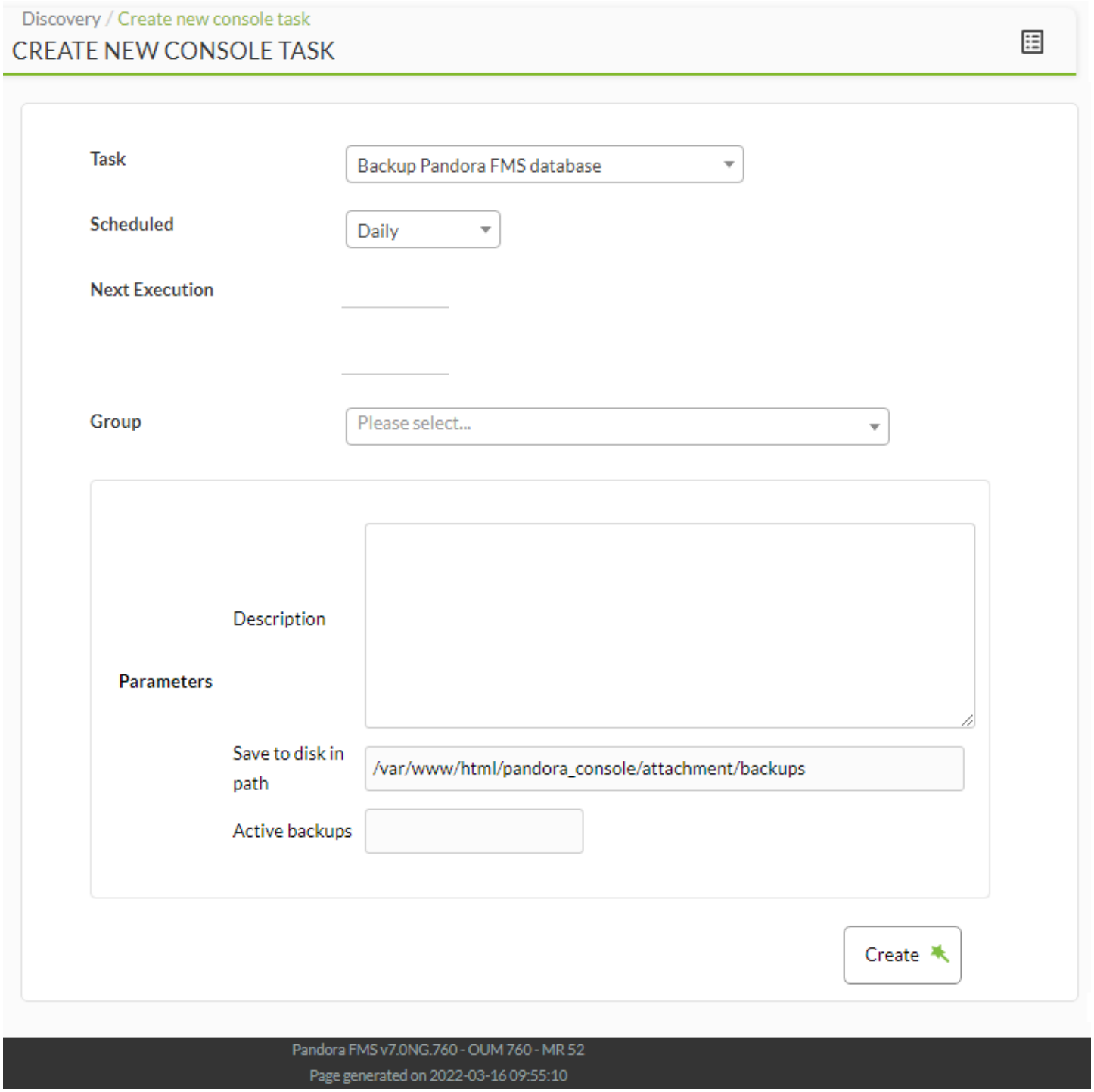


Общими полями для каждой задачи являются:

1. Scheduled: Периодичность выполнения задания, ежедневно (Daily), ежечасно (Hourly), ежемесячно (Monthly), только один раз (Not scheduled, см. следующий пункт), еженедельно (Weekly) и ежегодно (Yearly).
2. Next execution: При следующем выполнении задания выберите дату в первом поле и время во втором поле (всплывающее меню при нажатии на каждое).
3. Group: Группа, к которой будет принадлежать задание.

- Backup Pandora FMS database

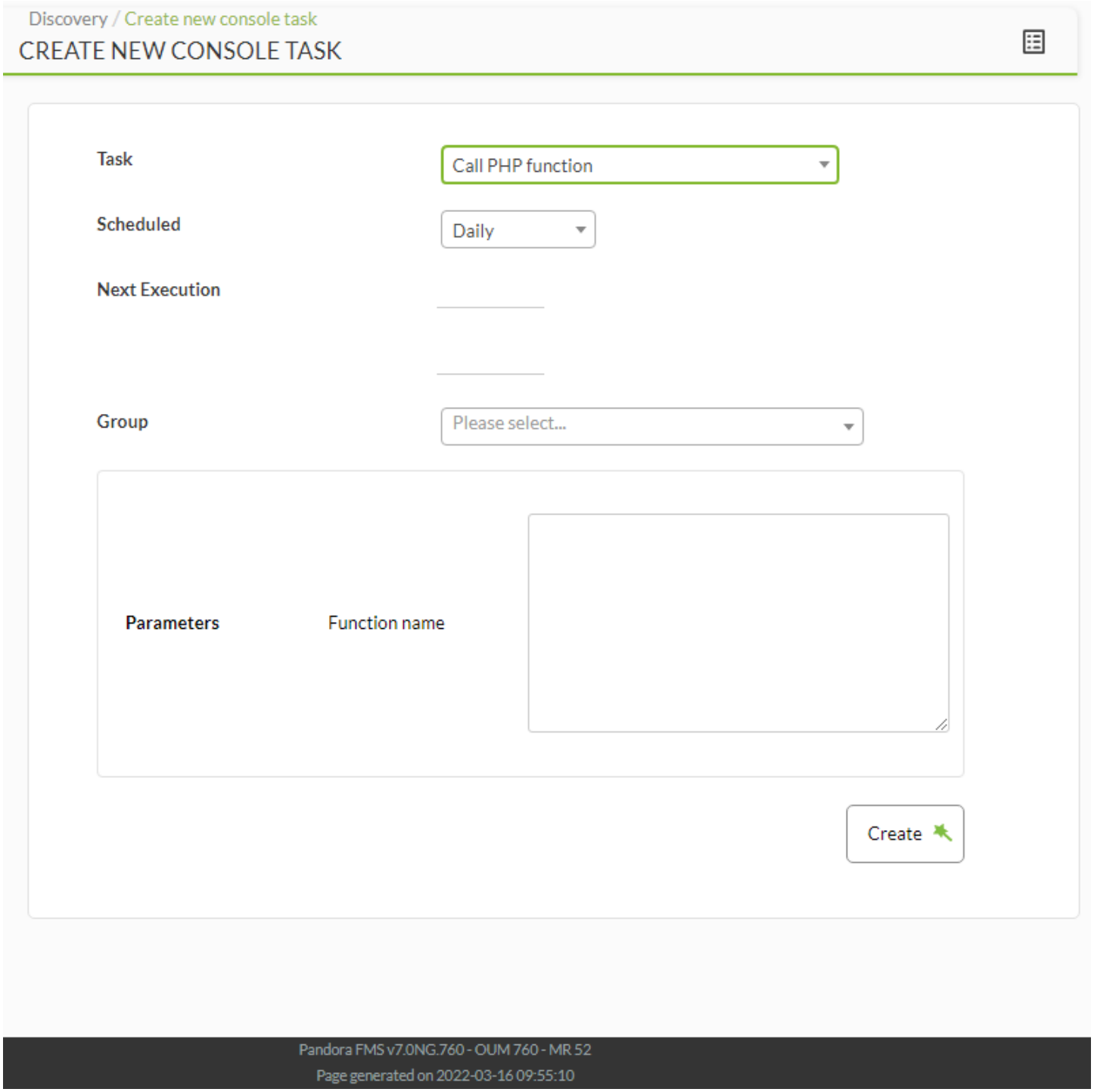
Задача резервного копирования базы данных Pandora FMS (*backup*):



Save to disk in path: Путь, на котором хранится резервная информация.

- Call PHP function

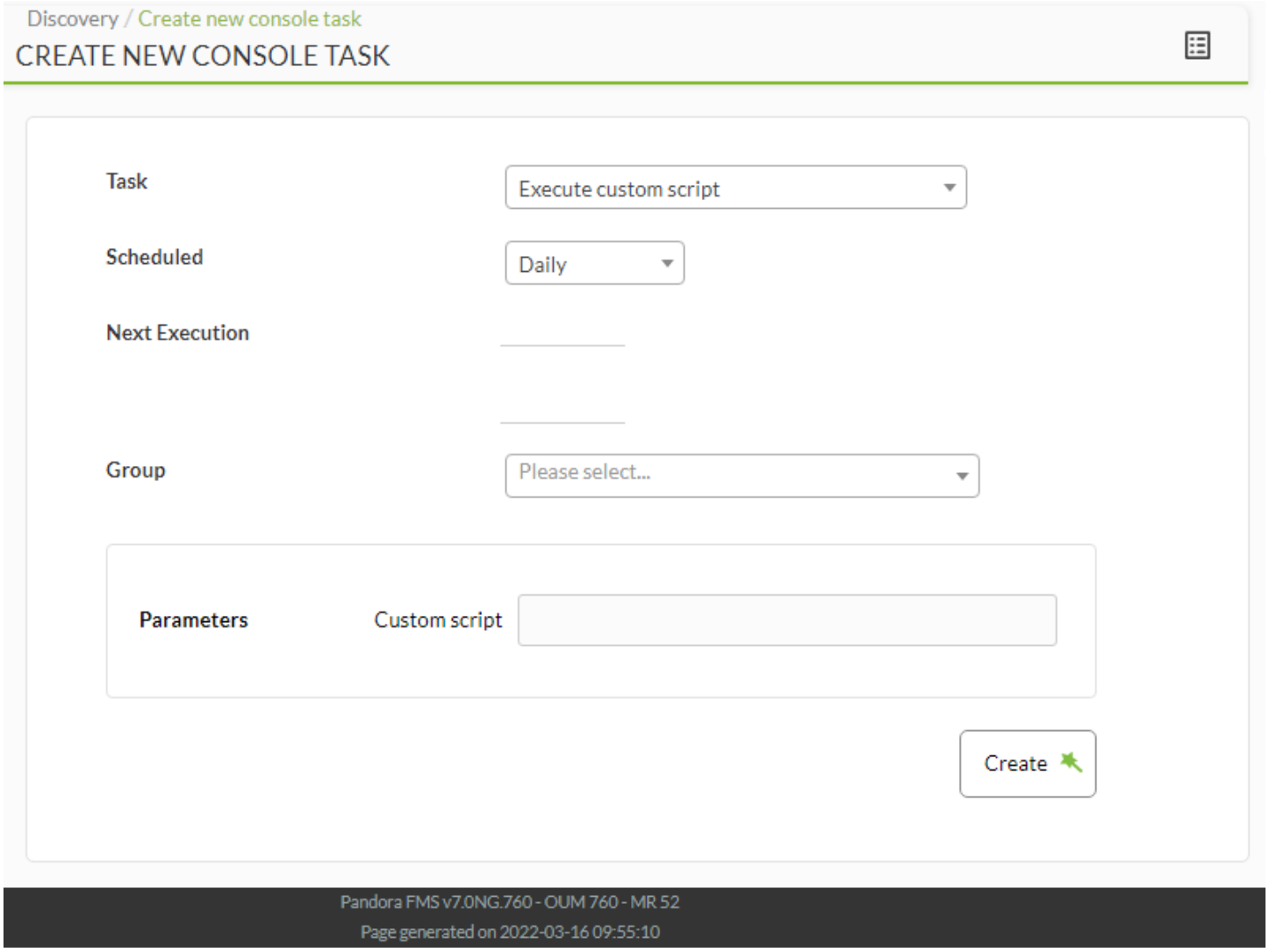
Задача выполнения функции, написанной на языке PHP:



Function name: Имя функции PHP, которая будет выполняться однократно или периодически.

- Execute custom script

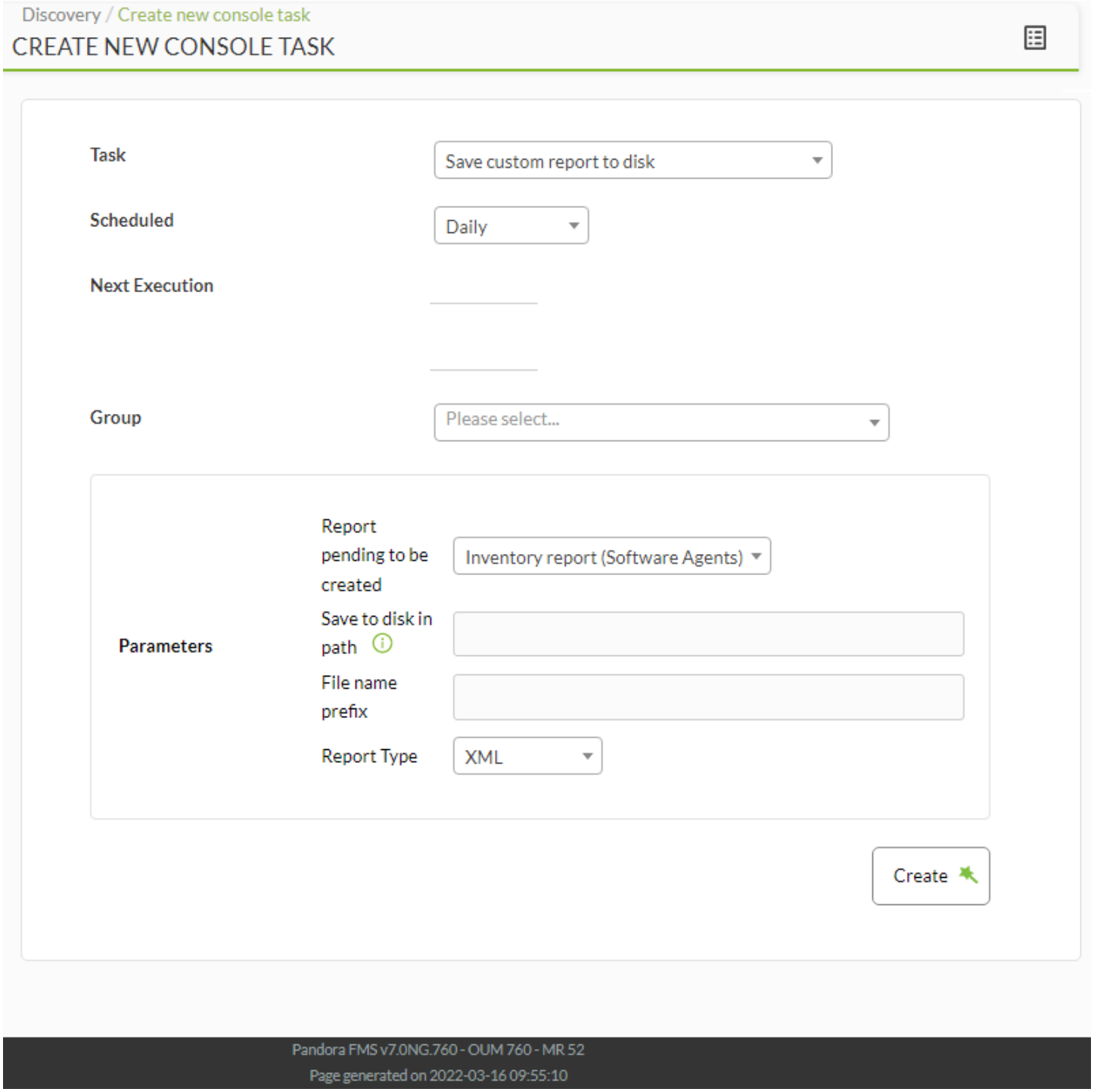
Задание на выполнение сценария:



Custom script: Имя сценария для запуска.

- Save custom report to disk

Индивидуальная задача создания и сохранения отчетов:



Report pending to be created: Пользовательский отчет (выпадающий список), на основе которого будет создан этот отчет. См. раздел «Создание (пользовательского) отчета».

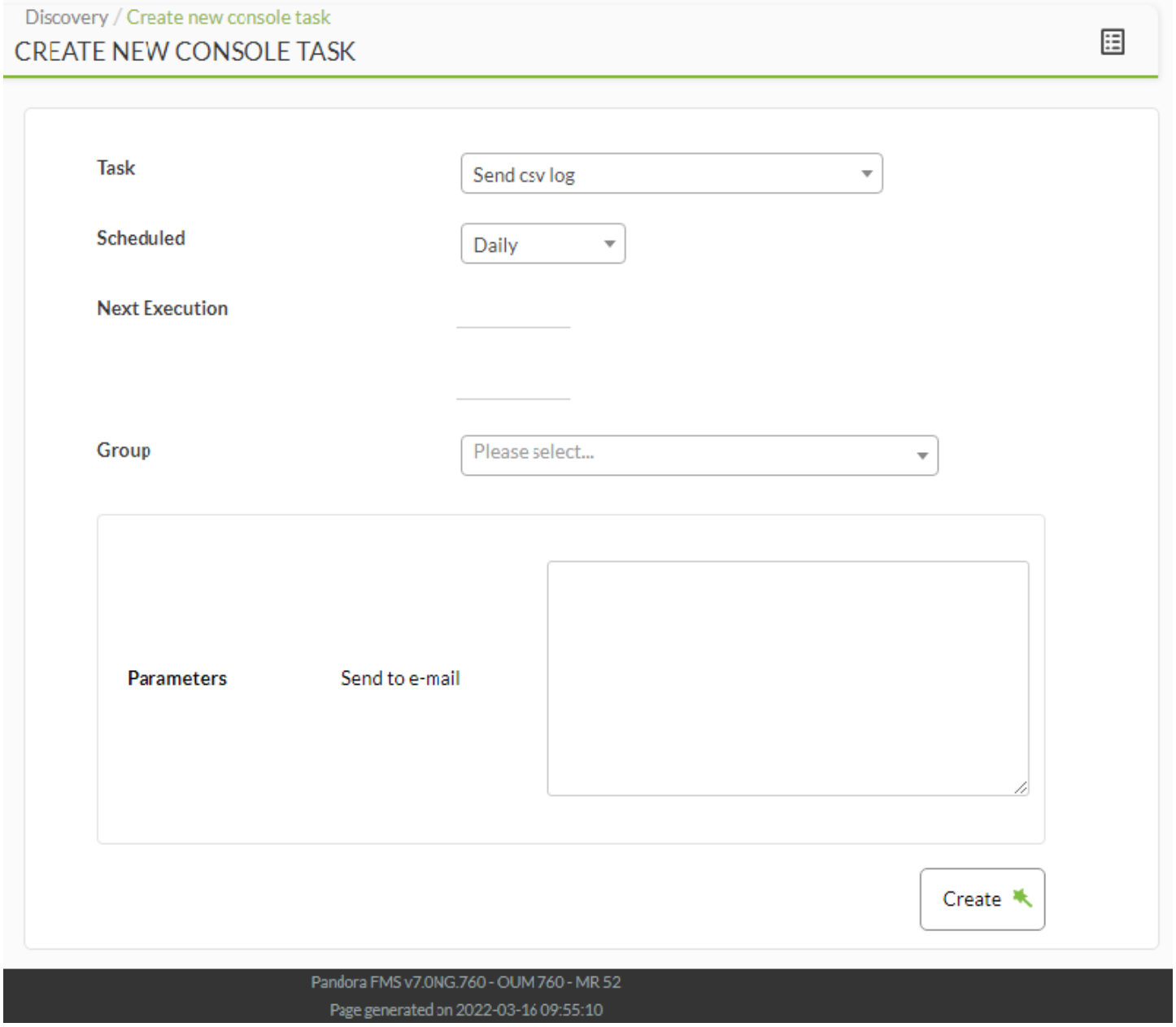
Save to disk in path: Путь, где будет храниться созданный отчет (пользователь apache должен иметь права на чтение и запись в этот каталог).

File name prefix: Префикс имени для последовательных отчетов.

Report Type: Сохраняется в формате XML, PDF, JSON о CSV.

- Send csv log

Задача отправки журналов событий в формате CSV по электронной почте.



Send to e-mail: Почтовый ящик, на который следует отправлять журналы событий в формате CSV.

- Send custom report (from template) by email

Отчеты (созданные на основе шаблона) для отправки по электронной почте:

Discovery / Create new console task

CREATE NEW CONSOLE TASK

Task Send custom report (from template) by e-...

Scheduled Daily

Next Execution

Group Please select...

Parameters

Template pending to be created: None

Agents: None, 1, 10, 100, 101, 102, 103, 104, 105, 106

Regexp agent filter

Report per agent: No

Report name

Send to e-mail addresses (separated by a comma)

Subject: This is an optional field

Message: This is an optional field

Report Type: XML

Create

Отчеты, которые должны быть отправлены по электронной почте:

- Индивидуальный шаблон для создания отчета,Template pending to be created.
- Информация об агентах для отчета, Agents; если вы хотите генерировать отдельные отчеты для каждого Агента, Report per agent.
- Адреса электронной почты для отправки отчета, Send to email addresses.
- Тема отправляемого письма, Subject.
- Тело сообщения, с которым будут отправлены отчеты, Message .
- Тип отчета, который будет отправлен, Report Type.

- Send custom report by email

Отчеты должны быть отправлены по электронной почте:

Discovery / Create new console task

CREATE NEW CONSOLE TASK

Task Send custom report by e-mail

Scheduled Daily

Next Execution

Group Please select...

Parameters

Report pending to be created: GitLab 9533

Send to e-mail addresses (separated by a comma):

Subject: This is an optional field

Message: This is an optional field

Report Type: XML

Create

Настраиваемый отчет (см. «Создание отчета») для создания отчета, Report pending to be created.

Информация об агентах для отчета, Agents; если вы хотите генерировать отдельные отчеты для каждого отчета, Report per agent.

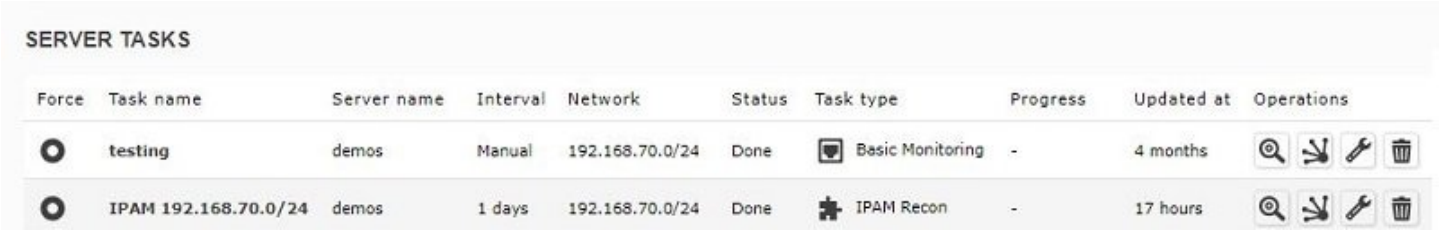
Почтовые адреса (через запятую) для отправки отчета, Send to email addresses.

Тема отправляемого письма, Subject.

Тело сообщения, с которым будут отправлены отчеты, Message .

Тип отправляемого отчета, Report Type.

Server tasks



Для каждой задачи *task*:

- Force: Принудительное выполнение.
- Task name: Имя Задачи.
- Server name: Сервер, который ее выполняет.
- Interval: Интервал времени, в течение которого она будет выполняться.
- Network: Сеть, где будут проводиться проверки.
- Status: Статус.
- Task type: Тип Задачи.
- Progress: Прогресс, если находится в работе.
- Updated at: Последнее обновление.
- Operations: Значки позволяют выполнять такие действия, как редактирование или удаление задания и др. Начиная с версии NG 752, при просмотре задач можно включить или отключить каждую задачу используя иконку.

Операции

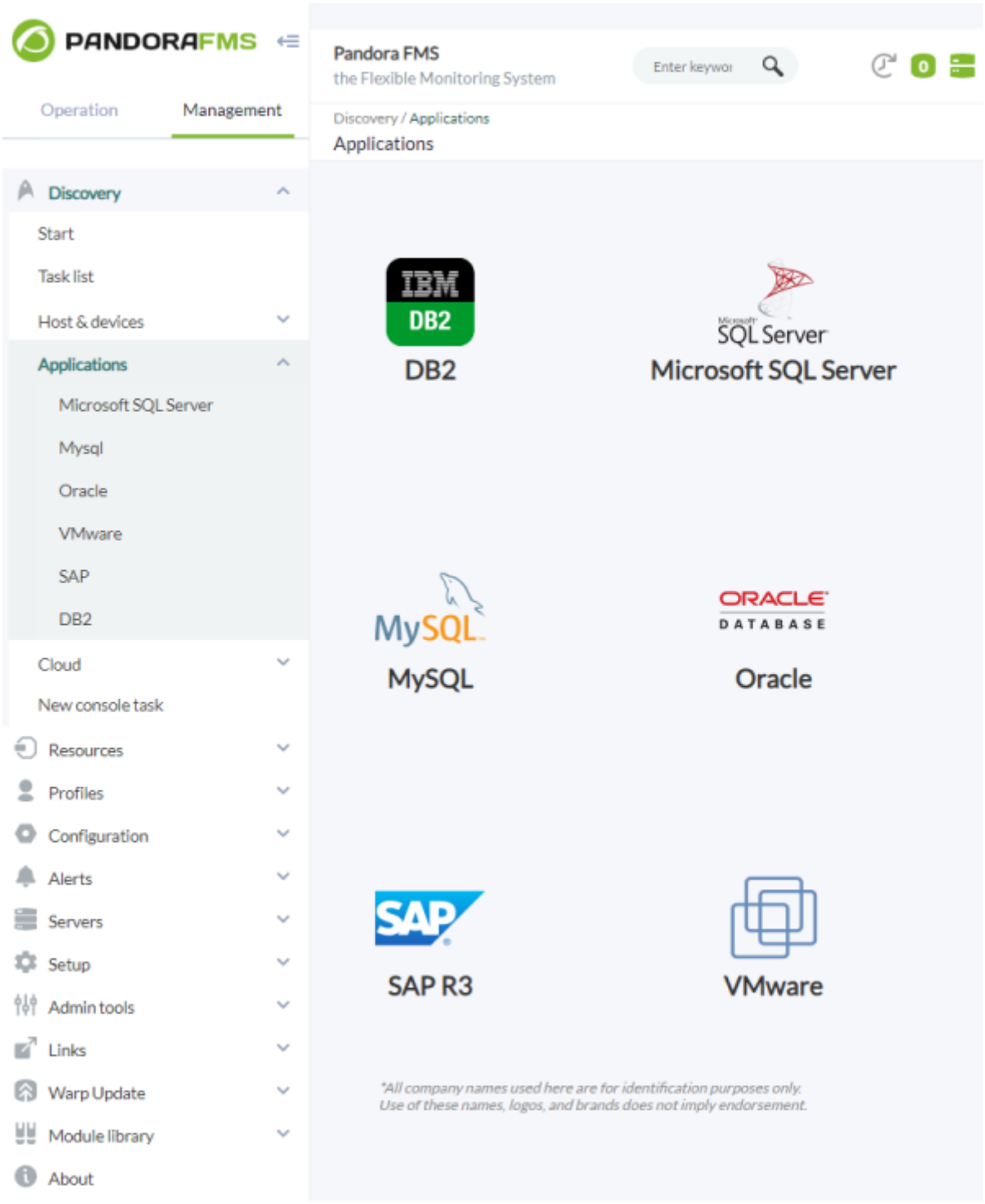
Редактирование задач распознавания сервера:

- Interval: Интервал выполнения задания, вручную или заданный.
- Task name: Имя Задачи.
- Discovery server: Servidor que la ejecutará, parámetro obligatorio.
- Network: Сервер, выполняющий задачу, обязательный параметр.
- Group: Группа.

- Comment: Соответствующие комментарии.

Discovery Applications

Вернуться к началу ♦



С помощью Pandora FMS можно удаленно контролировать приложения, используя *Discovery Applications*.

Discovery Applications: DB2

Версия NG 747 или выше.

Для мониторинга мотора реляционной базы данных DB2® от IBM® мы используем Официальный клиент IBM, а точнее пакет `ibm_data_server_driver_package_linuxx64_v11.5.tar.gz`. После загрузки пакета следуйте приведенным ниже инструкциям, чтобы распаковать и установить его:

```
tar -zxvf ibm_data_server_driver_package_linuxx64_v11.5.tar.gz
```

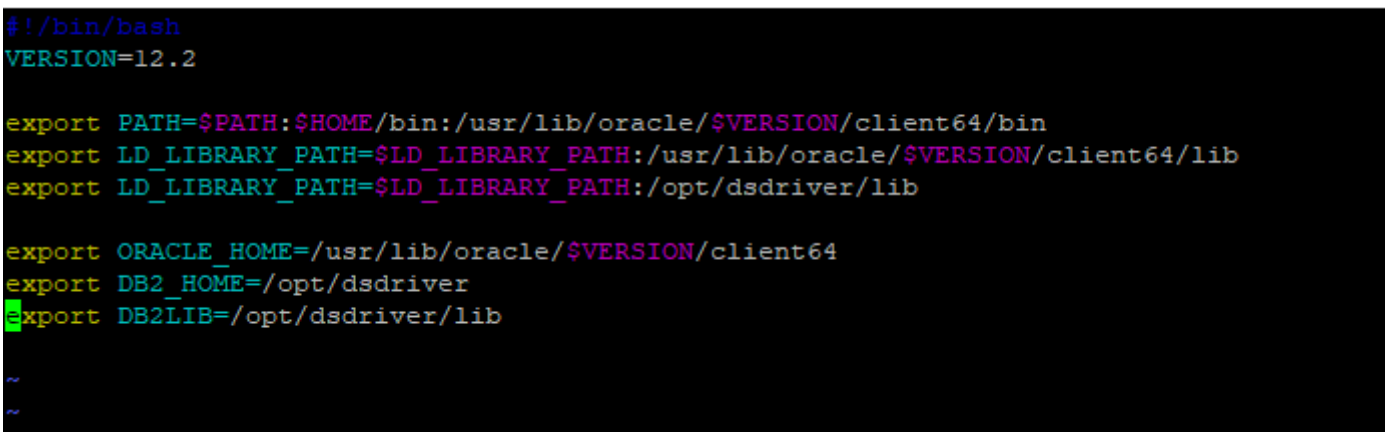
Переместите файл в каталог, куда вы хотите его установить. (ej. `/opt/dsdriver`).

```
mv PATH/ibm_data_server_driver_package_linuxx64_v11.5 /opt/dsdriver/
 cd /opt/dsdriver
 bash installDSDriver
 export DB2_HOME=/opt/dsdriver
 export DB2LIB=/opt/dsdriver/lib
 cd /usr/lib64
 ln -s /opt/dsdriver/lib/* ./
```

В файле `/etc/pandora/pandora_server.env` необходимо установить следующие переменные:

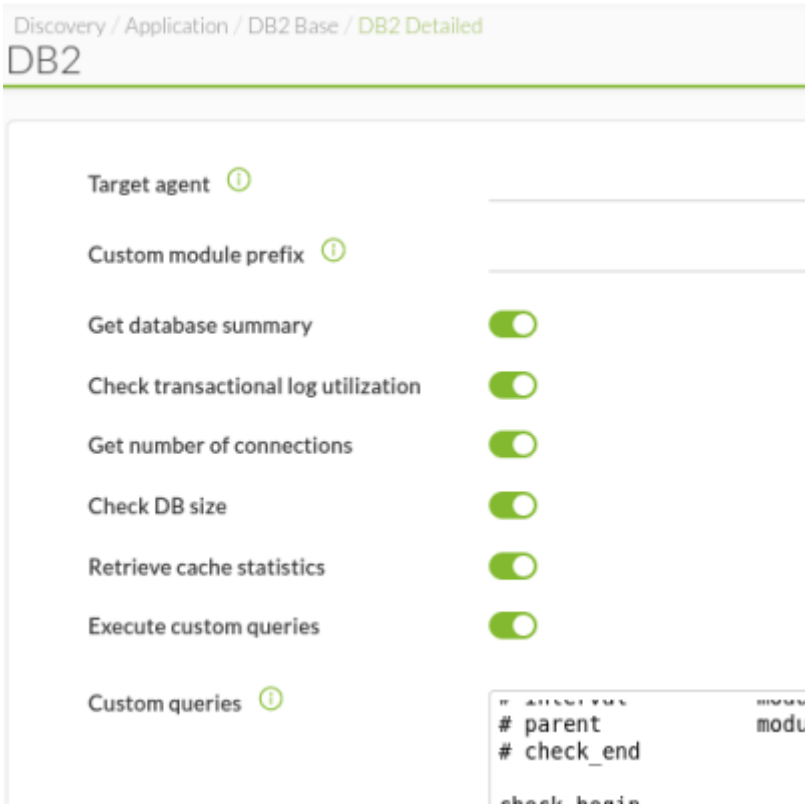
```
#!/bin/bash
 VERSION=12.2
 export PATH=$PATH:$HOME/bin:/usr/lib/oracle/$VERSION/client64/bin
 export LD_LIBRARY_PATH=$LD_LIBRARY_PATH:/usr/lib/oracle/$VERSION/client64/lib
 export LD_LIBRARY_PATH=$LD_LIBRARY_PATH:/opt/dsdriver/lib

 export ORACLE_HOME=/usr/lib/oracle/$VERSION/client64
 export DB2_HOME=/opt/dsdriver
 export DB2LIB=/opt/dsdriver/lib
```

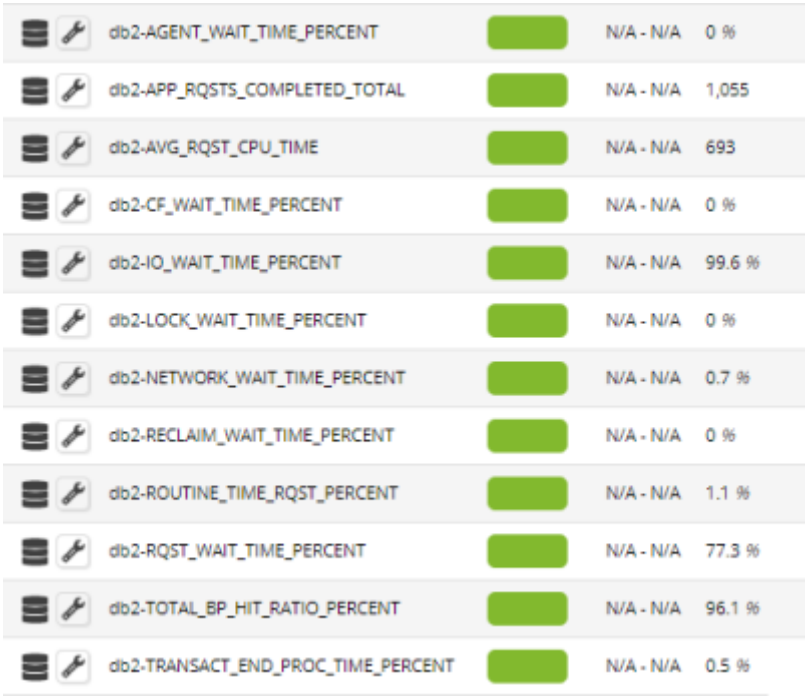


Версия может быть 11.x или 12.2 в зависимости от установленной системы.

Функции

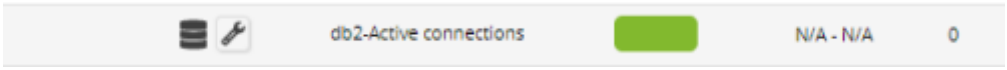


- Предопределенный модуль, обзор базы данных *Get database summary*:



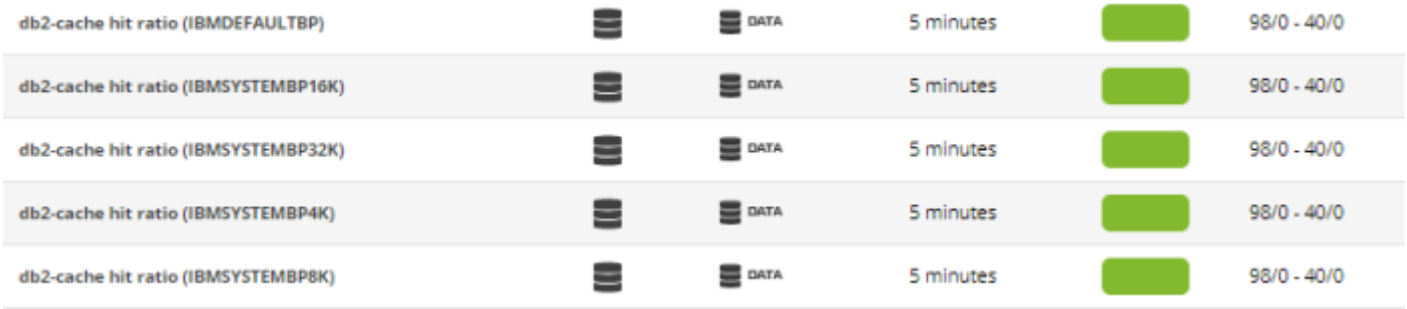
- Предопределенный модуль, *Check transactional log utilization*:

- Предопределенный модуль, *Number of connections*:

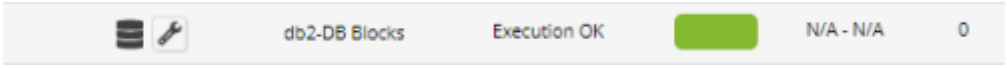


- Предопределенный модуль, *DB size*:

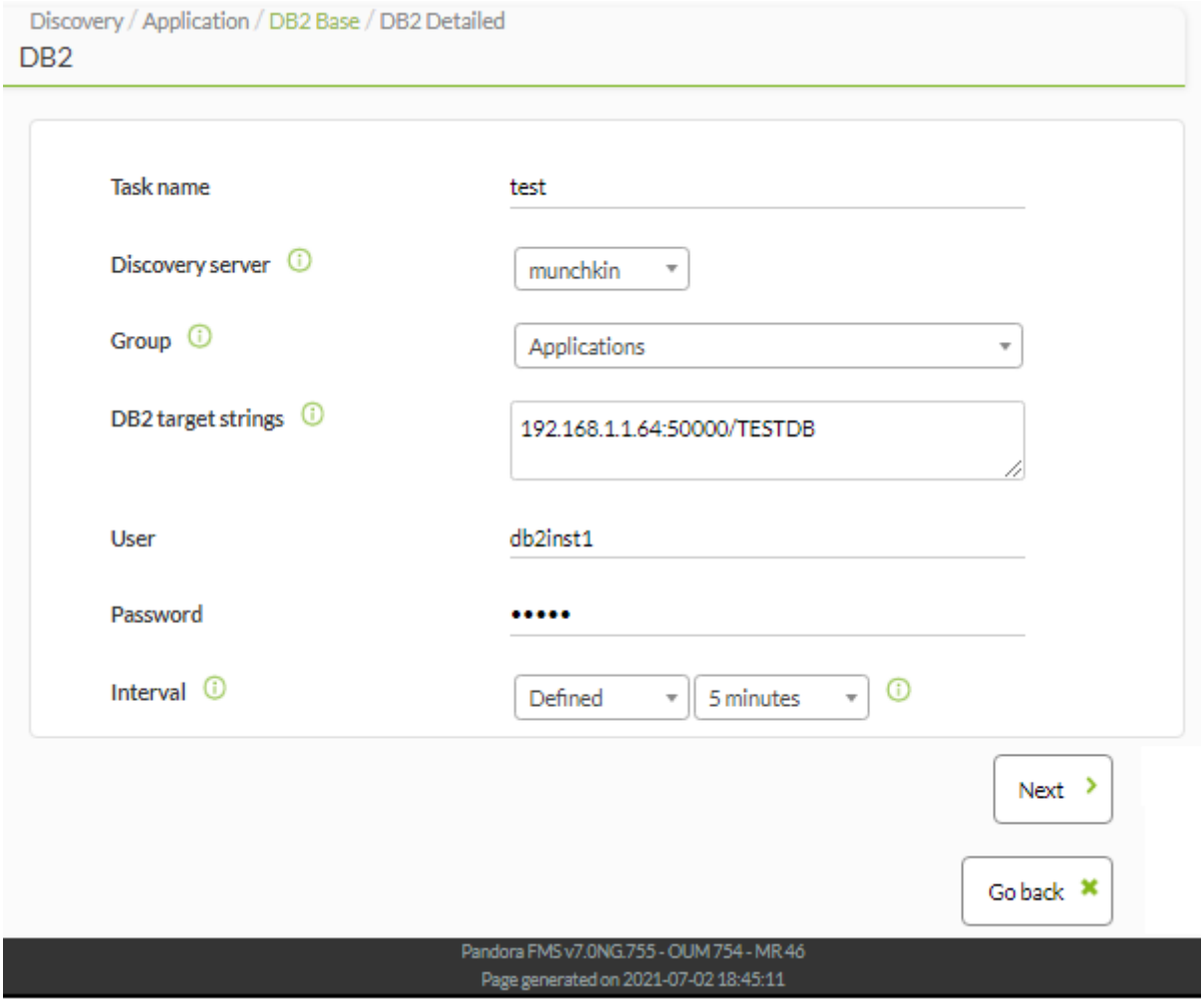
- Предопределенный модуль, *Retrieve cache statistics*:



- Модуль с помощью настраиваемых запросов:

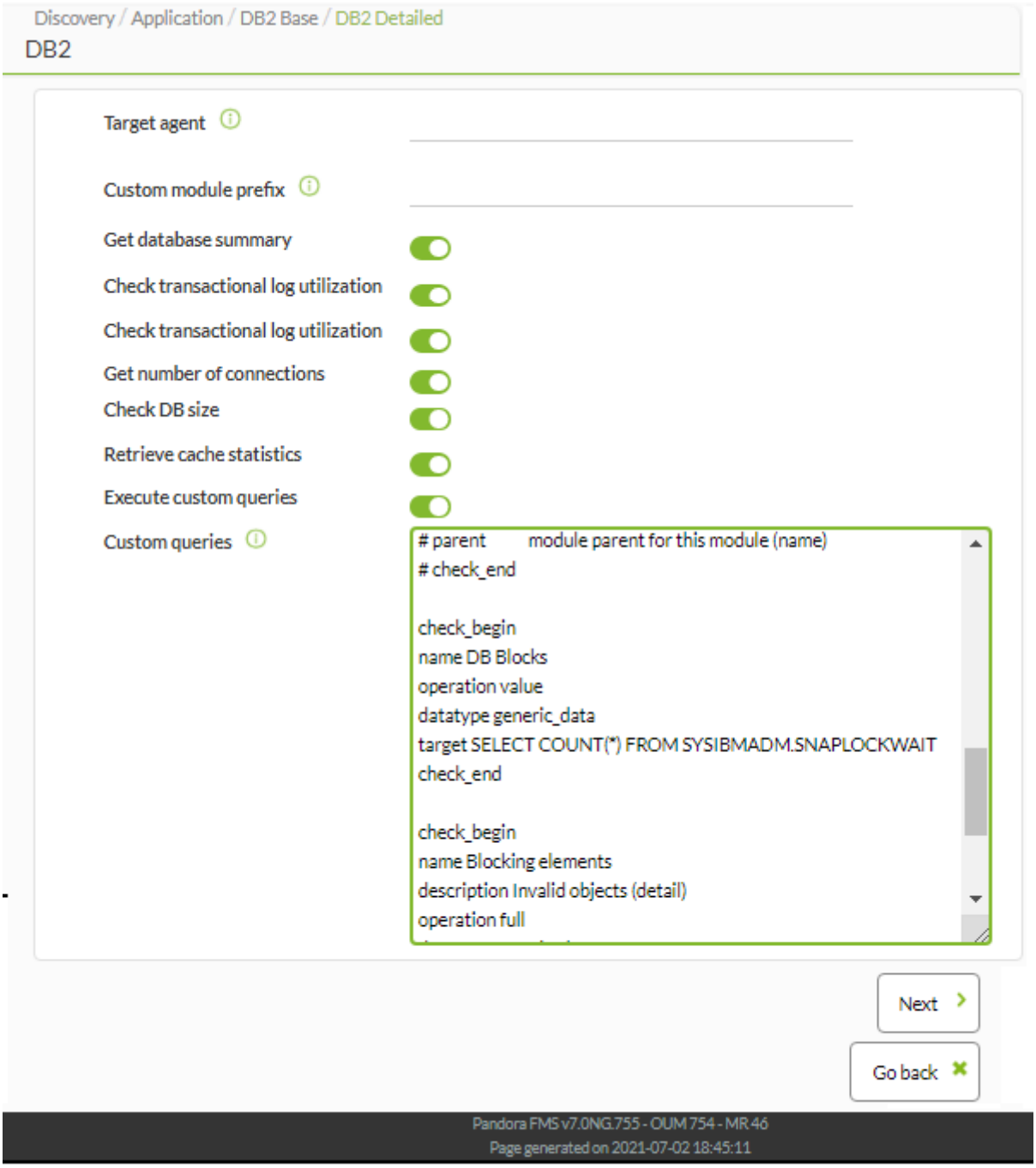


Чтобы выполнить этот пользовательский мониторинг, необходимо следовать шагам, которые дает помощник, для настройки задачи DB2®.



На первом этапе будут определены следующие параметры:

- Task name: Имя задачи.
- Discovery server: Сервер, выполняющий задачу мониторинга DB2®.
- Group: Группа, к которой принадлежат созданные агенты.
- DB2 target strings: Раздел, в котором определяется целевые *строки* нашей задачи. Мы можем добавить столько целевых IP-адресов, сколько захотим, разделяя их запятыми или линиями. Вы можете использовать # для комментариев.
- User: Пользователь DB2®, получающий доступ к мониторингу.
- Password: Пароль пользователя, определенный ранее.
- Interval: Интервал выполнения.



Во второй части конфигурации задачи указывается:

- Target agent: Агент, который будет получать информацию о мониторинге от DB2®. Если вы определяете несколько целевых *строк*, вы можете указать несколько имен в этом поле через запятую.
- Custom module prefix: Определяет пользовательский префикс, который будет сцеплен с именами модулей, создаваемых задачей.
- Get database summary: Возвращает сводку о состоянии базы данных.
- Check transactional log utilization: Указывает процент от общего пространства журнала, которое используется.
- Get number of connections: Возвращает количество соединений.
- Check DB size: Возвращает размер базы данных.
- Retrieve cache statistics: Возвращает статистику *кэша*.
- Execute custom queries: Выполняет пользовательские запросы.
- Custom queries: Позволяет определять пользовательские запросы.

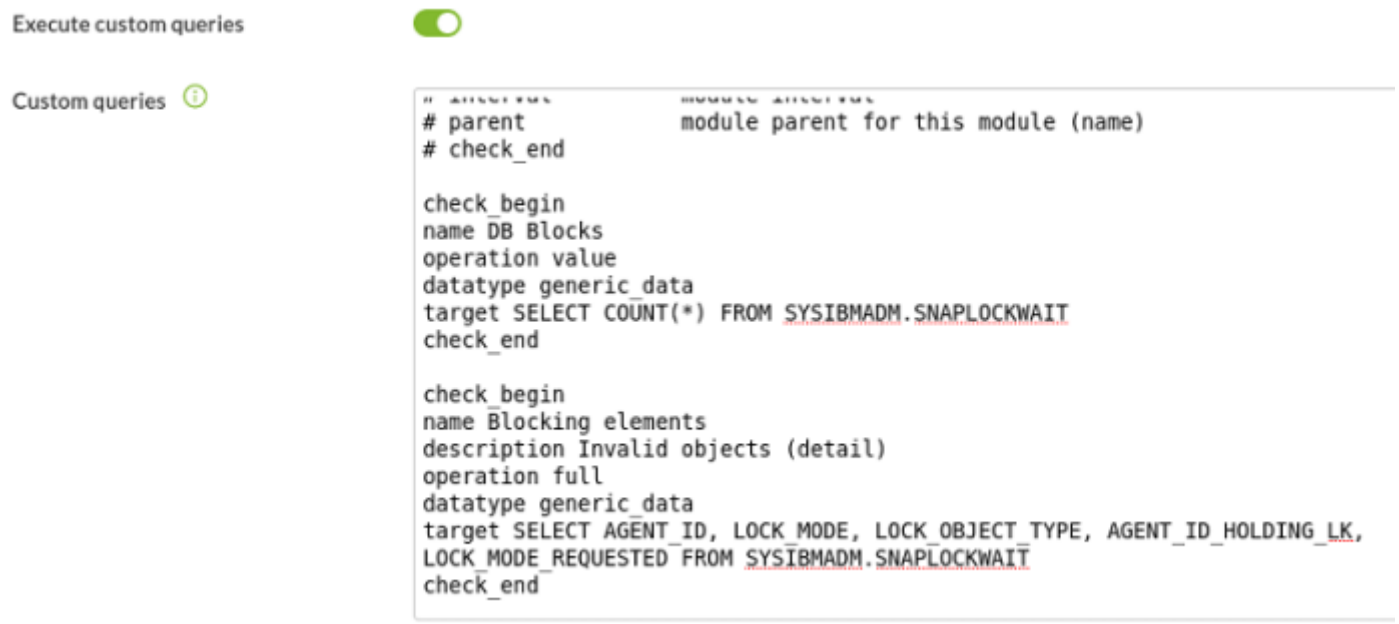
Пример

```
SELECT count(*) FROM SYSIBMADM.SNAPLOCKWAIT
```

возвращает информацию о моментальных снимках агентов базы данных, работающих от имени запросов, которые ожидают получения блокировок или *locks*. Следуя формату запроса:

```
SELECT * FROM <schema_name>.<table_name>
```

для этого типа базы данных мы сможем получить всевозможные модули.



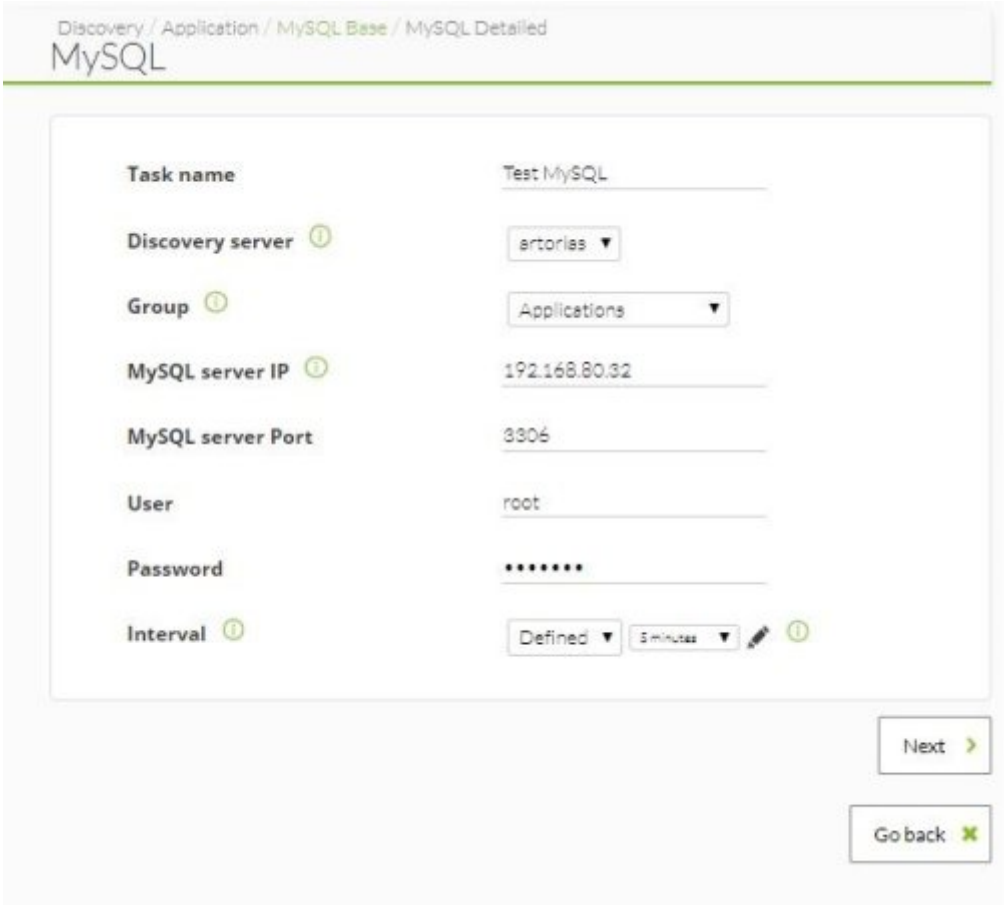
После выполнения описанных выше действий вы получите общий вид, аналогичный этому:

DB2 connection	DB2 availability		N/A - N/A	1
db2-Active connections			N/A - N/A	0
db2-AGENT_WAIT_TIME_PERCENT			N/A - N/A	0 %
db2-APP_RQSTS_COMPLETED_TOTAL			N/A - N/A	1,316
db2-AVG_RQST_CPU_TIME			N/A - N/A	650
db2-CF_WAIT_TIME_PERCENT			N/A - N/A	0 %
db2-Database size			N/A - N/A	88 *MB*
db2-DB Blocks	Execution OK		N/A - N/A	0
db2-IO_WAIT_TIME_PERCENT			N/A - N/A	99.3 %
db2-LOCK_WAIT_TIME_PERCENT			N/A - N/A	0 %
db2-Log utilization percent	Used 1 KB of 15488		N/A - N/A	0 %
db2-NETWORK_WAIT_TIME_PERCENT			N/A - N/A	0.9 %
db2-RECLAIM_WAIT_TIME_PERCENT			N/A - N/A	0 %
db2-ROUTINE_TIME_RQST_PERCENT			N/A - N/A	1 %
db2-RQST_WAIT_TIME_PERCENT			N/A - N/A	76.5 %
db2-TOTAL_BP_HIT_RATIO_PERCENT			N/A - N/A	96.9 %
db2-TRANSACT_END_PROC_TIME_PERCENT			N/A - N/A	0.5 %

Discovery Applications: MySQL

Версия NG 733 или выше.

Для задачи должны быть определены следующие параметры:



- Task name: Имя Задачи.
- Discovery Server: Сервер, который будет ее выполнять.
- MySQL server IP: IP-адрес сервера, на котором расположена среда MySQL®.
- MySQL server port: Порт предыдущего адреса.
- Interval: Период времени, в течение которого будет выполняться мониторинг.
- User: Пользователь MySQL®, под которым вы получаете доступ.
- Password: Пароль пользователя MySQL®, указанный выше.

Это должен быть пользователь с достаточными
правами на базу данных для выполнения запросов.

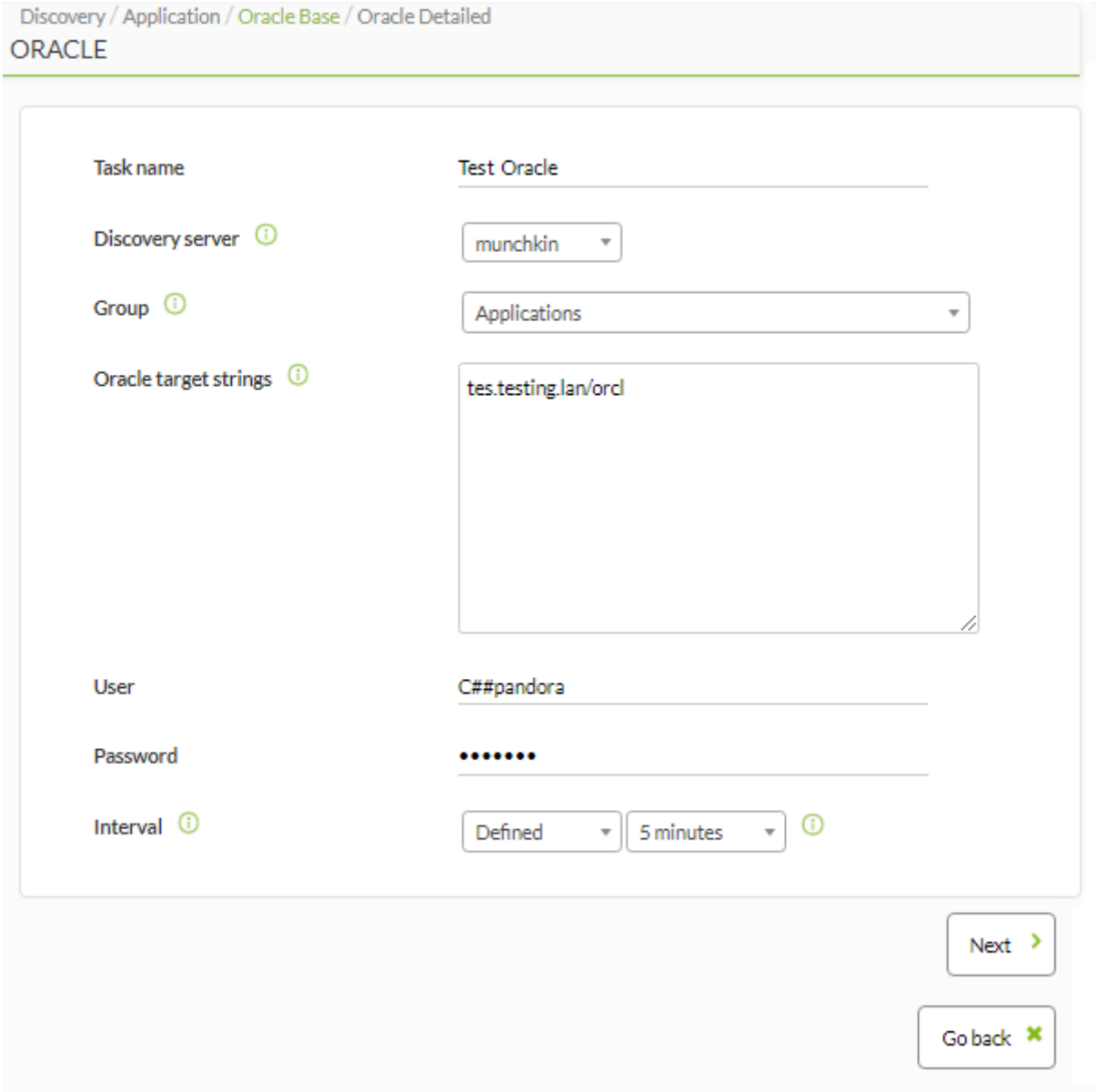
После завершения конфигурации необходимо указать модули:

- Target agent: Агент, на котором создаются модули.
- Custom module prefix: Определяет пользовательский префикс, который будет сцеплен с именами модулей, создаваемых задачей.
- Scan databases: Выполнит исследование баз данных и их объектов.
- Create agent per database: Он позволяет создать агента для каждой базы данных, найденной в соответствии с предыдущим пунктом.
- Check engine uptime: Проверит время работы MySQL®.
- Retrieve query statistics: Позволяет получить статистику выполненных запросов.
- Analyze connections: Информация о подключении.
- Retrieve InnoDB statistics: Возвращает статистику InnoDB.
- Retrieve cache statistics: Возвращает статистики кэша;.

- Custom queries: Позволяет определять пользовательские SQL-запросы.

Discovery Applications: Oracle

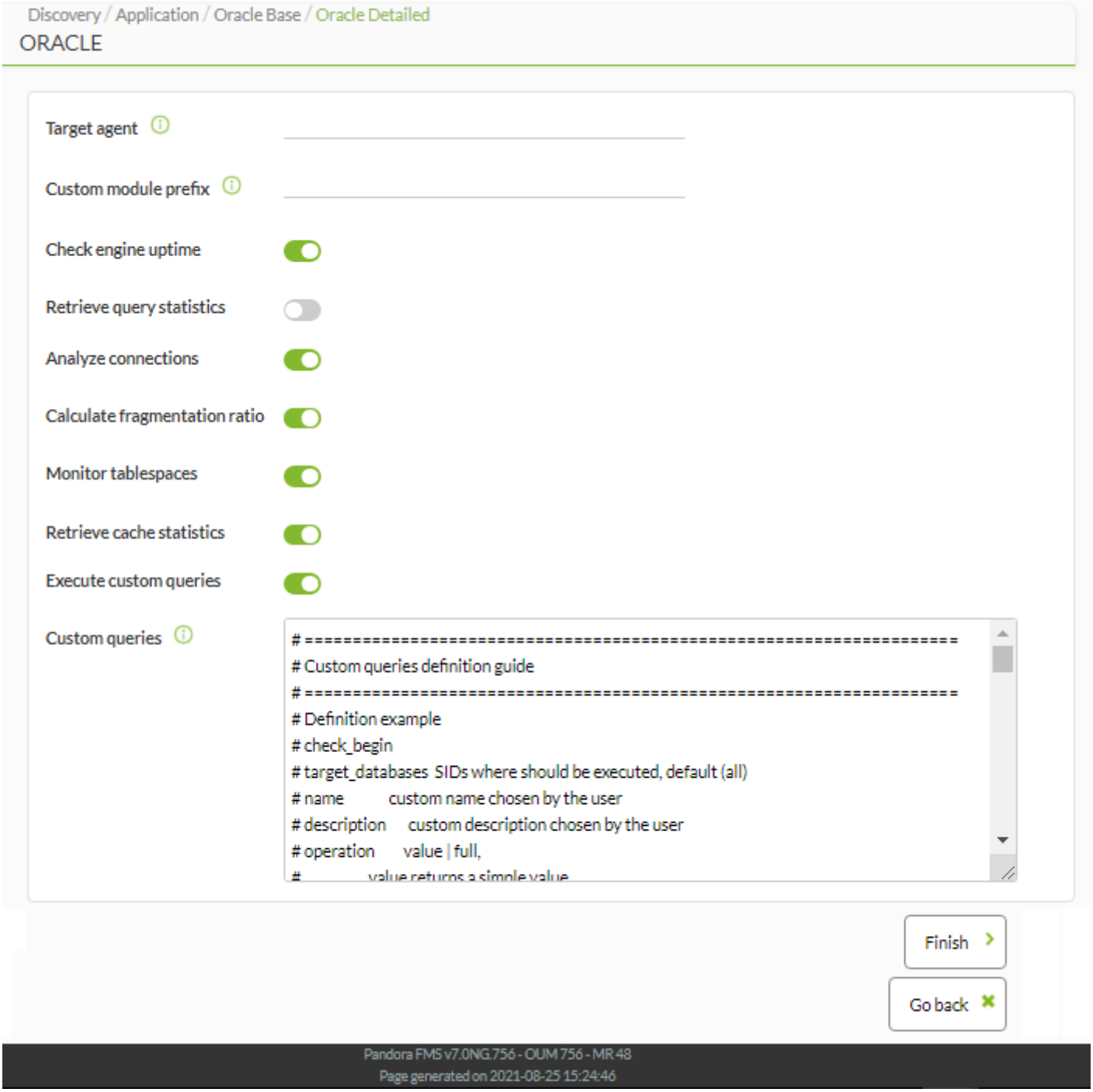
Версия NG 733 или выше.



Мониторинг Oracle® позволяет определить следующие параметры задачи:

- Task name: Имя Задачи.
- Discovery Server: Назначенный Сервер.
- Oracle target strings: Здесь определяются целевые *строки*.
- User: Пользователь Oracle®, получающий доступ к мониторингу.
- Password: Пароль пользователя, определенный ранее.
- Interval: Период времени для выполнения.

После того, как вы настроили вышеуказанные значения, следует перейти к выполнению следующих модулей задачи:



- Target agent: Агент, который будет получать данные. Если оставить пустым, он будет сгенерирован автоматически.
- Custom module prefix: Определяет пользовательский префикс, который будет сцеплен с именами модулей, создаваемых задачей.
- Check engine uptime: Время функционирования Oracle®.
- Retrieve query statistics: Статистики выполненных запросов. Если вы включите эту опцию, вам необходимо предоставить права доступа к таблице V$SQLSTATS.
- Analyze connections: Информация о подключении.
- Calculate fragmentation ratio: Вычисляет коэффициент фрагментации. Необходимо предоставить права доступа к таблице dba_tables.
- Monitor tablespaces: Проверяет структуры, содержащие данные в Oracle®.
- Retrieve cache statistics: Возвращает статистику *кэша*. Необходимо предоставить права доступа к таблицам v$librarycache и v$rowcache.
- Execute custom queries: Выполняет пользовательские запросы.
- Custom queries: Позволяет определять пользовательские запросы.

Важно: для выполнения запросов должны быть предоставлены необходимые разрешения; например:

```
CREATE USER pandora IDENTIFIED BY pandora;
GRANT CREATE SESSION TO pandora;
GRANT SELECT any dictionary TO pandora;
GRANT SELECT ON V_$SYSSTAT TO pandora;
GRANT SELECT ON V_$STATNAME TO pandora;
GRANT SELECT ON gv$sysstat TO pandora;
GRANT SELECT ON v$sesstat TO pandora;
GRANT SELECT ON V_$INSTANCE TO pandora;
GRANT SELECT ON V_$LOG TO pandora;
GRANT SELECT ON SYS.DBA_DATA_FILES TO pandora;
GRANT SELECT ON SYS.DBA_FREE_SPACE TO pandora;
GRANT SELECT ON V_$parameter TO pandora;
GRANT SELECT ON dba_tablespaces TO pandora;
GRANT SELECT ON dba_data_files TO pandora;
GRANT SELECT ON dba_free_space TO pandora;
GRANT SELECT ON V$SQLSTATS TO pandora;
GRANT SELECT ON dba_tables TO pandora;
GRANT SELECT ON v$librarycache TO pandora;
GRANT SELECT ON v$rowcache TO pandora;
.
.
(others GRANTs necessary, for all tables used in the plugin configuration file)
.
.
--
-- if somebody still uses Oracle 8.1.7...
GRANT SELECT ON sys.dba_tablespaces TO pandora;
GRANT SELECT ON dba_temp_files TO pandora;
GRANT SELECT ON sys.v_$Temp_extent_pool TO pandora;
GRANT SELECT ON sys.v_$TEMP_SPACE_HEADER TO pandora;
GRANT SELECT ON sys.v_$session TO pandora;
```

Установка пакетов Oracle

- Установить Oracle® Instant Client с веб-сайта Oracle®:

```
https://www.oracle.com/technetwork/database/database-technologies/instant-client/downloads/index.html
```

- Необходимые пакеты:

```
oracle-instantclient11.1-basic-11.1.0.7.0-1.x86_64.rpm
 oracle-instantclient11.1-devel-11.1.0.7.0-1.x86_64.rpm
 oracle-instantclient11.1-sqlplus-11.1.0.7.0-1.x86_64.rpm
```

- Подготовить загрузочную среду pandora_server:

В каталоге pandora_server необходимо создать файл pandora_server.env со следующей информацией, а затем выполнить его `./pandora_server.env`

```
# Set Oracle environment for pandora_server
cat> /etc/pandora/pandora_server.env <<'EOF_ENV'
#!/bin/bash
VERSION=11.1
export PATH=$PATH:$HOME/bin:/usr/lib/oracle/$VERSION/client64/bin
export LD_LIBRARY_PATH=$LD_LIBRARY_PATH:/usr/lib/oracle/$VERSION/client64/lib
export ORACLE_HOME=/usr/lib/oracle/$VERSION/client64
EOF_ENV
```

- Следует перезапустить pandora_server

```
/etc/init.d/pandora_server restart
```

Если вы используете пакет E7, вы должны установить библиотеку и переменные среды версии 12.2, а также использовать пакеты Oracle®. (v12.2)

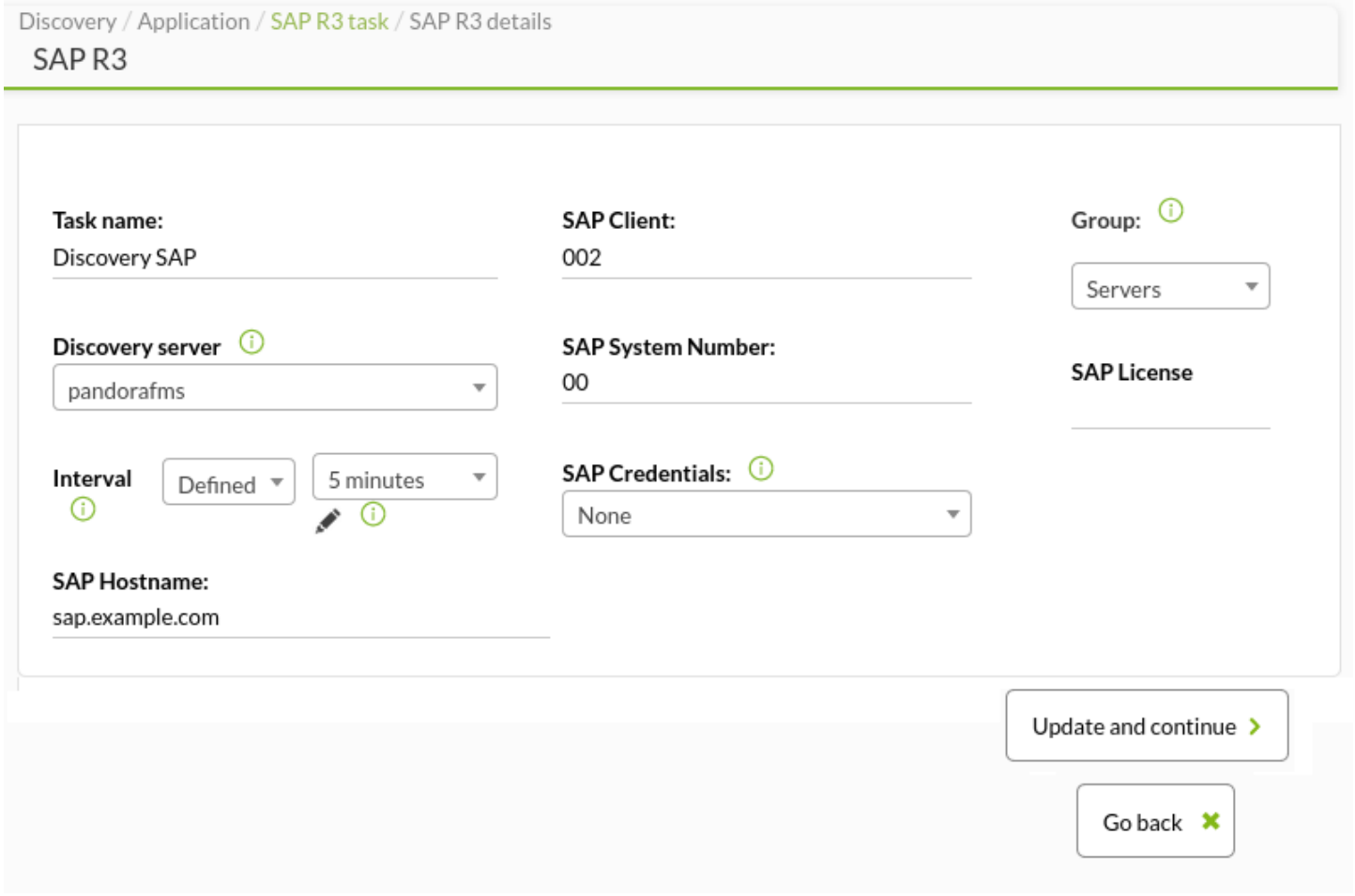
Начиная с версии NG 754, доступны дополнительные опции для ручного запуска и выключения сред High Availability (HA).

Discovery Applications: SAP

Версия NG 741 или выше.

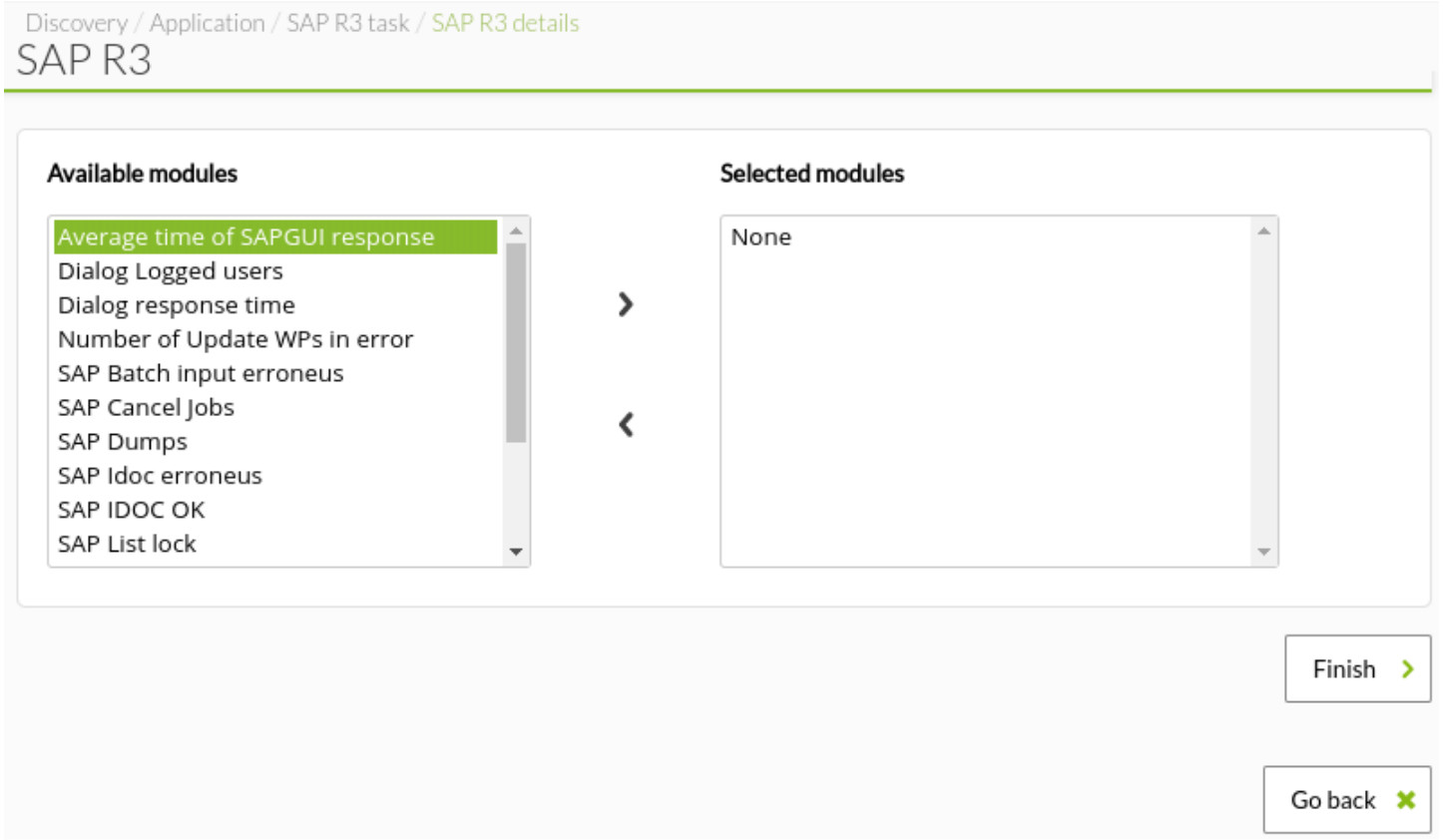
Система проведет вас через каждый шаг, чтобы настроить SAP в соответствии с вашими потребностями. Вы можете узнать больше из обучающего видеоролика «Мониторинг SAP с помощью Pandora FMS Discovery». Одна и та же задача может быть определена для мониторинга систем с аналогичной конфигурацией.

Если вам нужно контролировать различные конфигурации, вы должны создать задачу для каждой конфигурации.



Чтобы иметь возможность использовать SAP в Discovery, необходимо настроить специальный номер лицензии для этого *плагина*, который не входит в лицензию Pandora FMS Enterprise. Вы должны настроить эту лицензию в Setup → Enterprise.

Вы должны выбрать из списка информацию о системе SAP, которую вы хотите восстановить:



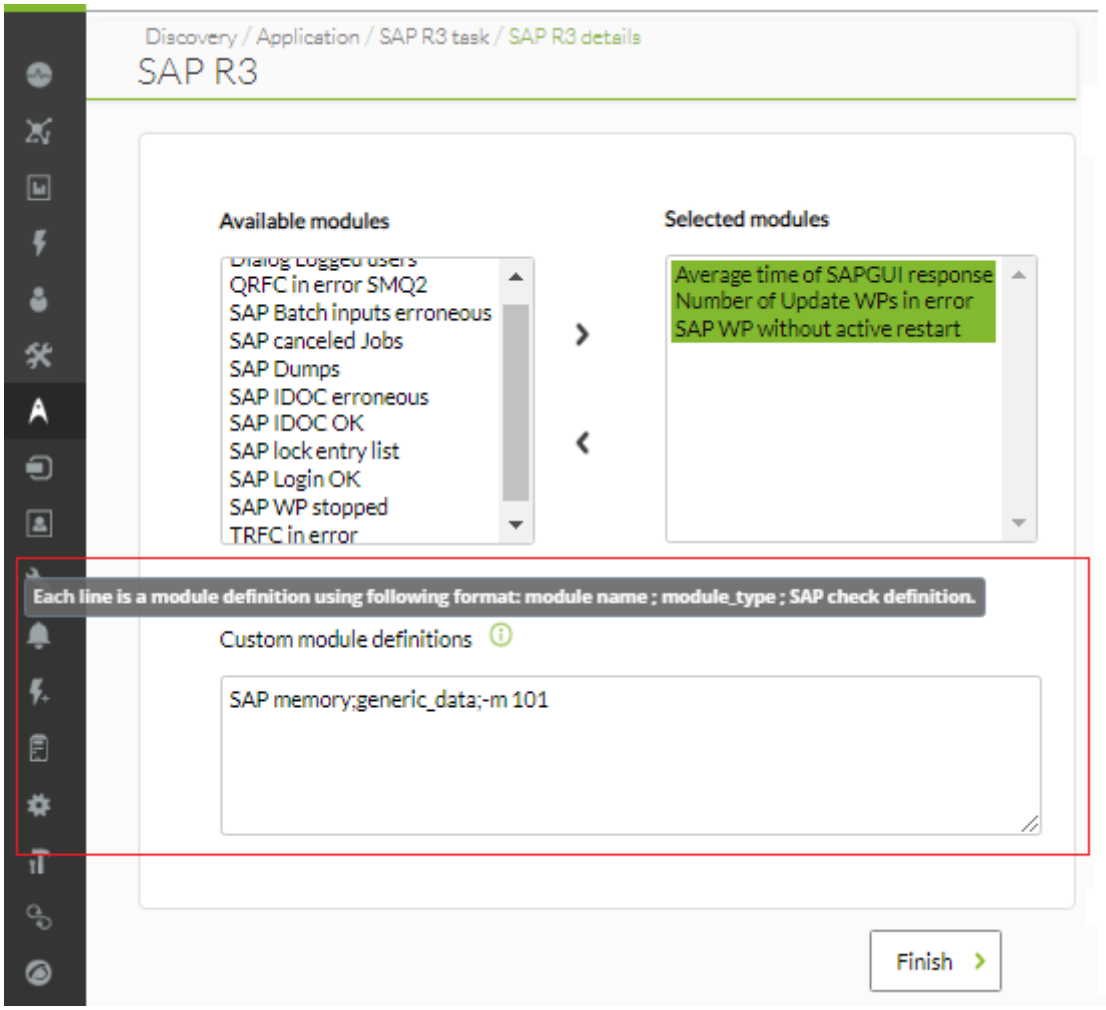
Pandora FMS Discovery будет отвечать за сбор информации, храня ее в агентах, представленных *SAP Hostnames*, которые вы определили.

Если вы устанавливаете Pandora FMS из пакетов или ваша система старше версии NG741, вы должны развернуть официальный плагин SAP на сервере Pandora FMS и настроить его вручную в соответствии с разделом Ручная установка коннектора Discovery для SAP.

Пользовательский SAP

Версия NG 747 или выше.

Помимо доступных модулей (Available modules) в Pandora FMS, вы можете добавить множество дополнительных модулей через раздел пользовательских определений модулей. (Custom module definitions).



Каждая добавляемая строка должна иметь следующий формат, с использованием точки с запятой в качестве разделителя полей:

<имя модуля>; <тип модуля>; <определение проверки SAP>

Пример ознакомления с информацией в системе SAP:

```
SAP info;generic_data_string;-m 120
```

Вы можете добавить столько пользовательских модулей, сколько вам нужно, а затем продолжить процесс таким же образом, как описано в предыдущем разделе.

Ручная установка коннектора SAP Discovery Connector

Если у вас установлена более старая версия NG 741, необходимо загрузить коннектор и настроить его вручную.

- Установите JAVA (JRE) на сервере Pandora FMS.
- Загрузите коннектор или удаленный //plugin// для Linux с сайта SAP.
- Настройте файл `pandora_server.conf` и установите следующие параметры:

```
# Discovery SAP
 java /usr/bin/java

 # Discovery SAP utils
 sap_utils /usr/share/pandora_server/util/recon_scripts/SAP
```

- В каталоге, указанный с помощью *token* конфигурации `sap_utils` распакуйте файлы *tarball*, загруженные из библиотеки под названием «Pandora FMS SAP Discovery for Linux» и содержащие следующие файлы:

```
Deset_SAP_Plugin.jar
 dev_jco_rfc.trc
 libsapjco3.so
 sapjco3.dll
 sapjco3.jar
```

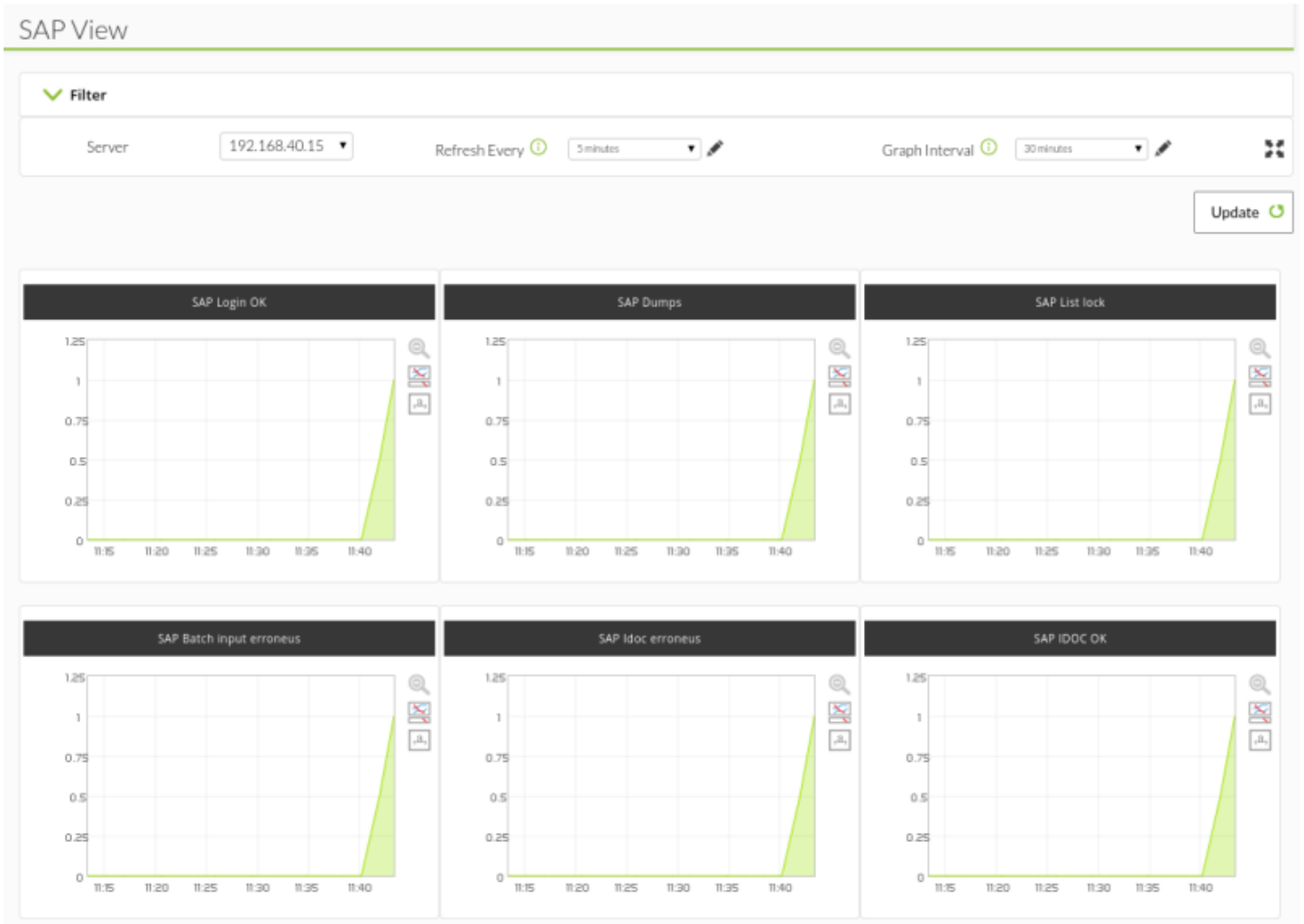
- Перезапустите сервер pandora_server

```
/etc/init.d/pandora_server restart
```

Начиная с версии NG 754 и выше, доступны дополнительные опции по ручному запуску и выключению сред высокой доступности (HA).

SAP View

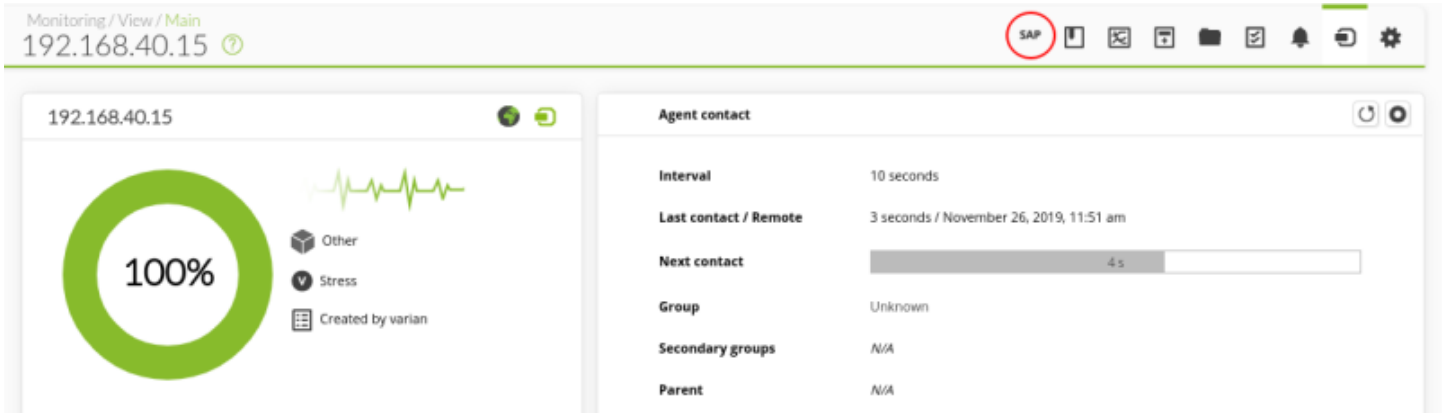
Позволяет отобразить общее состояние серверов SAP:



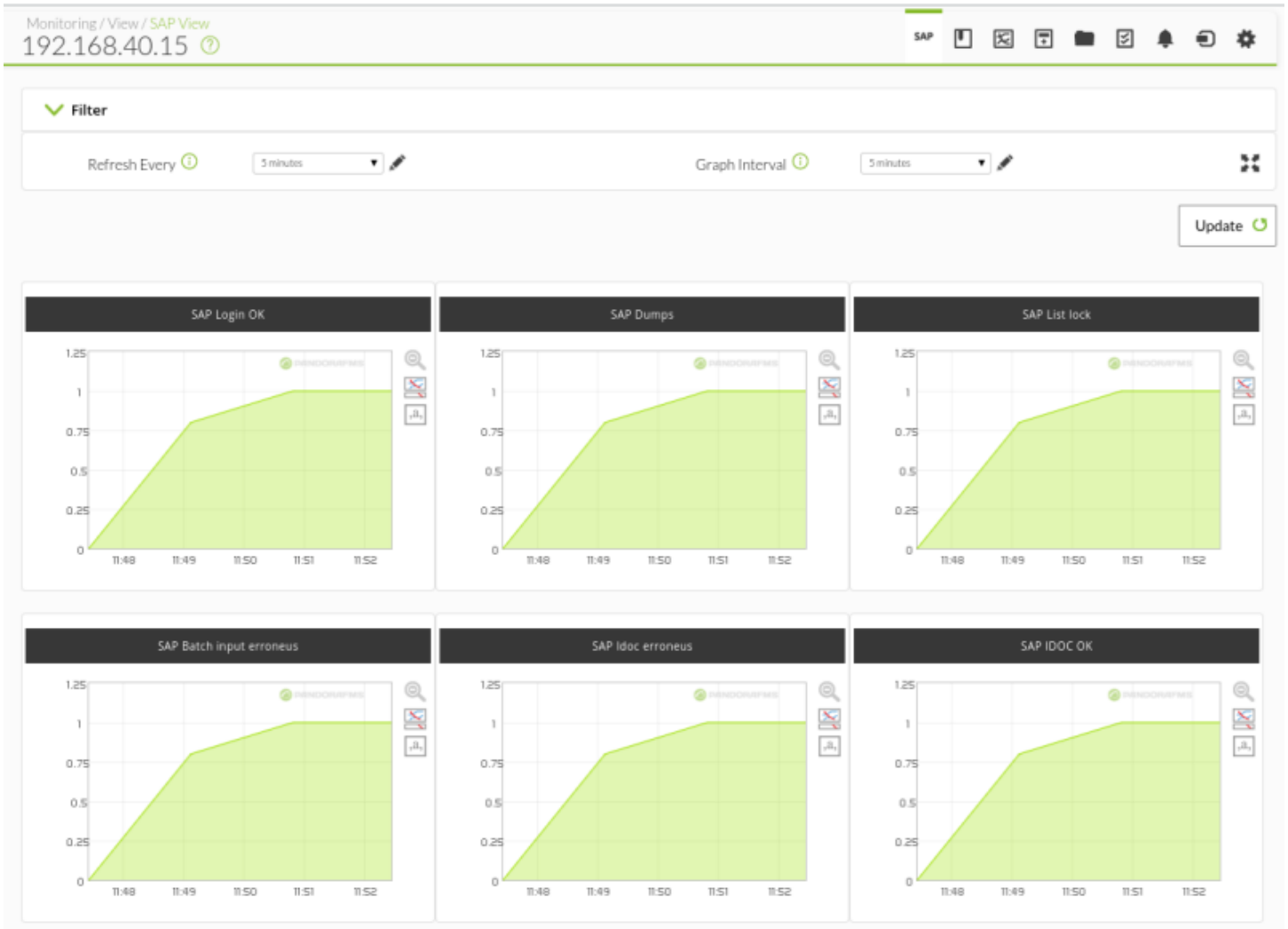
В этом представлении отображается панель с доступными модулями SAP выбранного агента SAP. Вы можете выбрать время обновления и интервал для отображения на графиках.

Специальный вид SAP

Вид SAP также интегрирован в виде новой вкладки при просмотре агента. Если система обнаружит, что агент является агентом SAP, откроется доступ к вкладке SAP View:

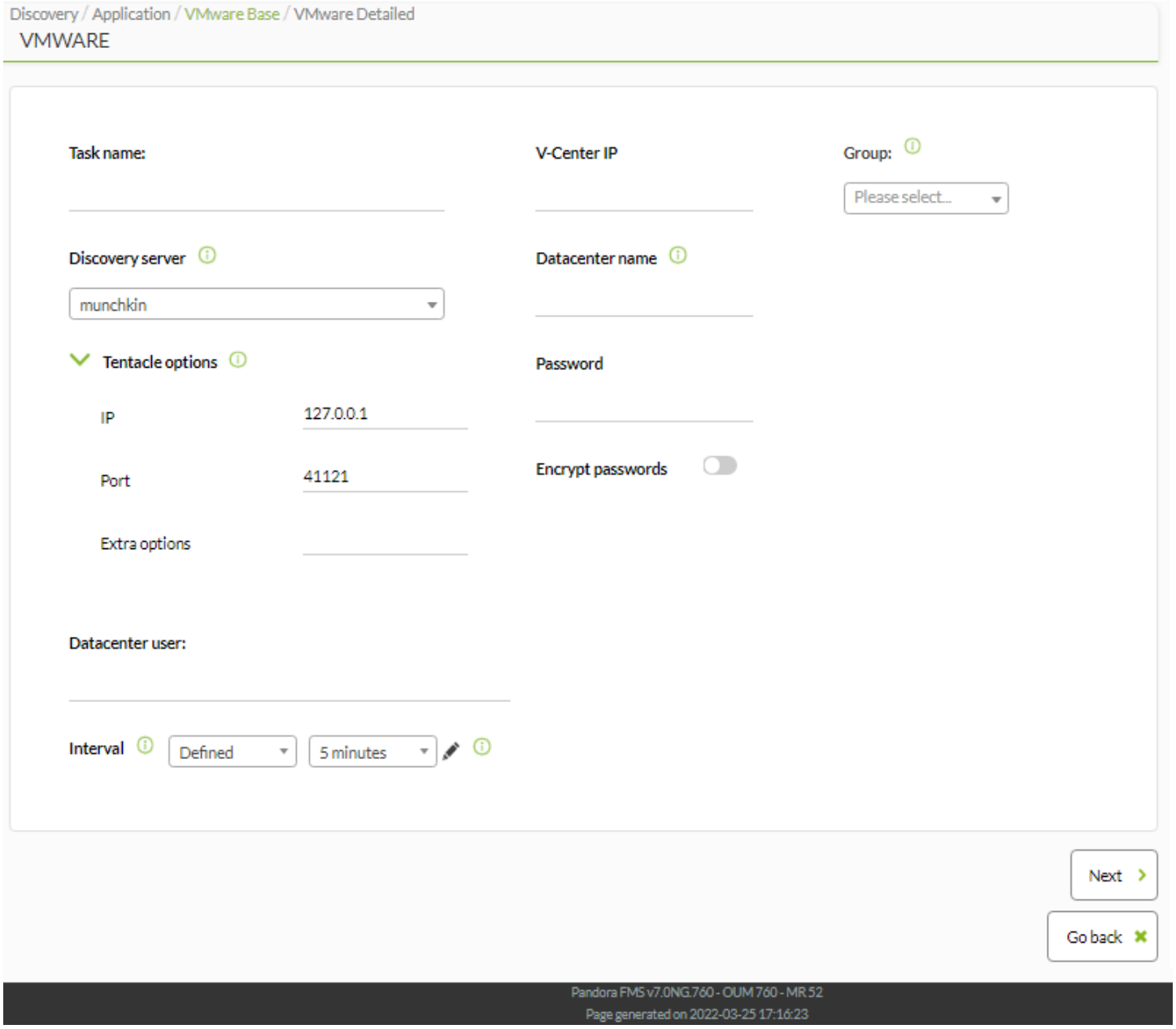


В виде агента будет представлен обзор состояния модулей SAP текущего агента:



Discovery Applications: VMware

Версия NG 732 или выше. Более подробную информацию вы можете получить в видеоуроке «Мониторинг VMWare с помощью Pandora FMS Discovery».



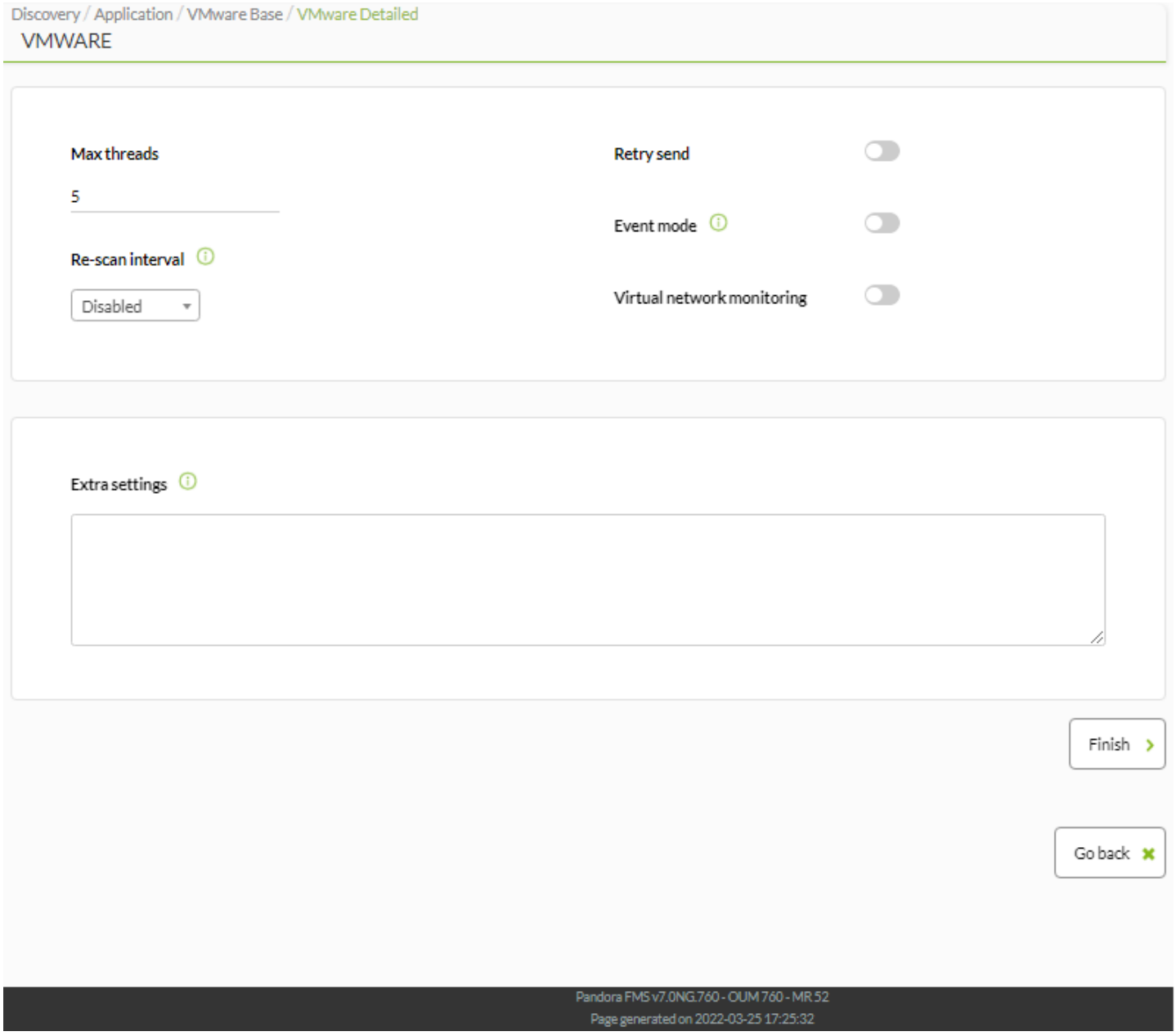
Вы должны указать:

- Имя для идентификации задачи, Task name.
- Discovery Server для его запуска.
- IP-адрес, V-Center IP.
- Имя *datacenter*, которое можно получить с экрана администрирования установки VMware.
- Пользователь и пароль с правами на чтение; только для этого помощника можно включить шифрование пароля, Encrypt passwords.
- Время мониторинга Interval.
- Группа, с которой будут связаны агенты, созданные задачей VMware.

Следует учитывать, что если на сервере Pandora FMS активен токен *autocreate_group*, он отдаст приоритет группе, соответствующей указанному ID, вместо применения конфигурации мастера.

В случае ручной установки или обновления с версии Pandora FMS, предшествующей 732, необходимо будет установить SDK для корректной работы VMWare.

После завершения базовой конфигурации укажите следующее:



- Max threads: Количество потоков, использующих *скрипт* мониторинга VMware для ускорения сбора данных.
- Retry send: Повторная попытка в случае ошибки.
- Event mode: (Только для VCenter) обеспечивает мониторинг на основе событий VMware VCenter. Этот режим является уникальным и независимым от стандартного мониторинга.
- Virtual network monitoring: Включает мониторинг виртуальных сетевых устройств, определенных в VMware.
- Extra settings: Любые дополнительные параметры, необходимые для настройки мониторинга VMware, должны быть включены здесь в текстовом режиме.

Посмотрите раздел Мониторинг виртуальных сред с помощью VMware для получения дополнительной информации.

Discovery Applications: MS SQL

Pandora FMS позволяет осуществлять мониторинг баз данных Microsoft SQL Server®. Для этого необходимо установить Open Database Connectivity (ODBC) от Microsoft® в системе, где работает сервер Pandora FMS.

Начиная с версии NG 753 вы должны использовать пакеты Enterprise Alternative Server packages для совместимости с Perl.

Как установить Microsoft ODBC

- Для CentOS 7:

```
curl https://packages.microsoft.com/config/rhel/7/prod.repo \
> /etc/yum.repos.d/mssql-release.repo && \
   yum remove unixODBC-utf16 unixODBC-utf16-devel && \
   ACCEPT_EULA=Y yum install -y msodbcsql17
```

- Для CentOS 8:

```
curl https://packages.microsoft.com/config/rhel/8/prod.repo \
 > /etc/yum.repos.d/mssql-release.repo && \
    yum remove unixODBC-utf16 unixODBC-utf16-devel && \
    ACCEPT_EULA=Y yum install -y msodbcsql17
```

Вам следует проверить файл конфигурации сервера Pandora FMS.

```
/etc/pandora/pandora_server.conf
```

Находясь в файле конфигурации, найдите следующий токен:

```
mssql_driver <CADENA IDENTIFICATIVA>
```

Параметр `<CADENA IDENTIFICATIVA>` указан в `/etc/odbcinst.ini`, который был создан при установке ODBC.

По умолчанию эта строка имеет вид:

```
ODBC Driver 17 for SQL Server
```

Настроить задачу Discovery Applications MS SQL

Чтобы создать задачу мониторинга для базы данных Microsoft SQL Server, необходимо получить к ней доступ через Discovery (Discovery → Applications → Microsoft SQL Server).

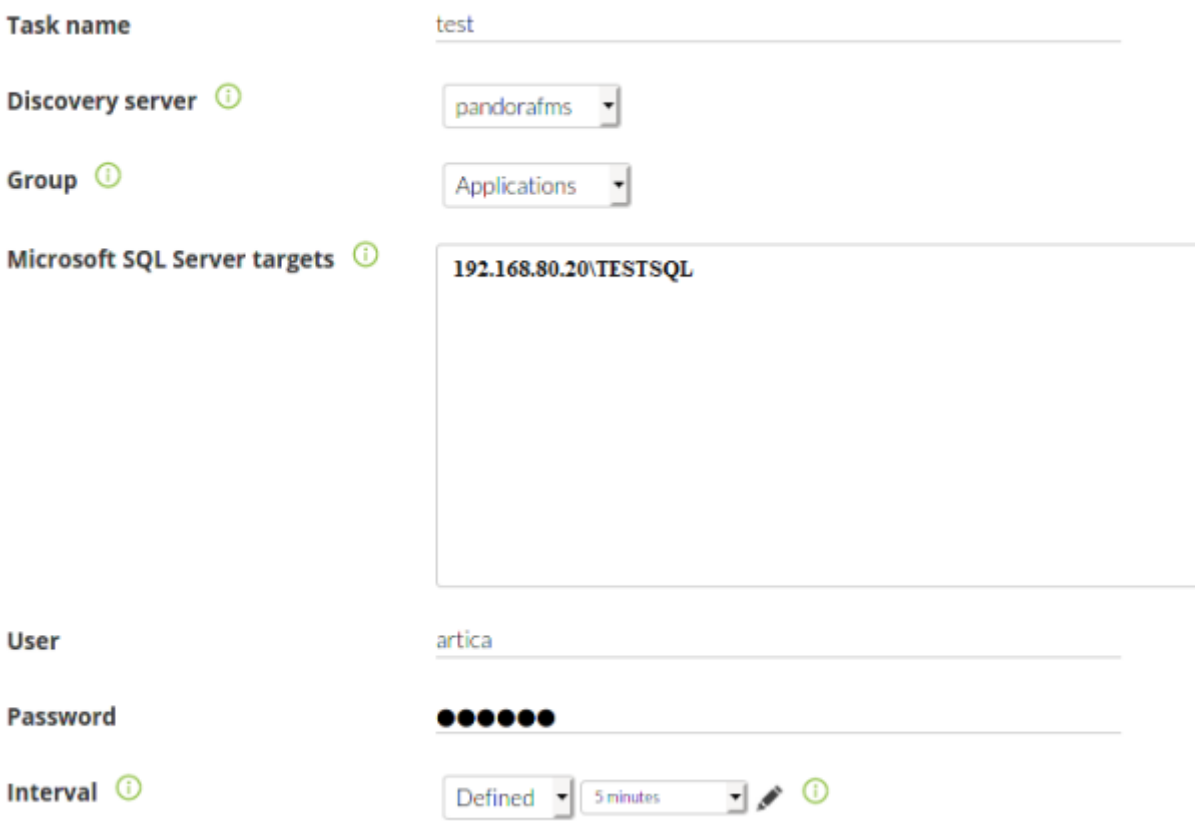
После выбора задачи Microsoft SQL Server® необходимо определить экземпляры:

```
IP\Instancia
```

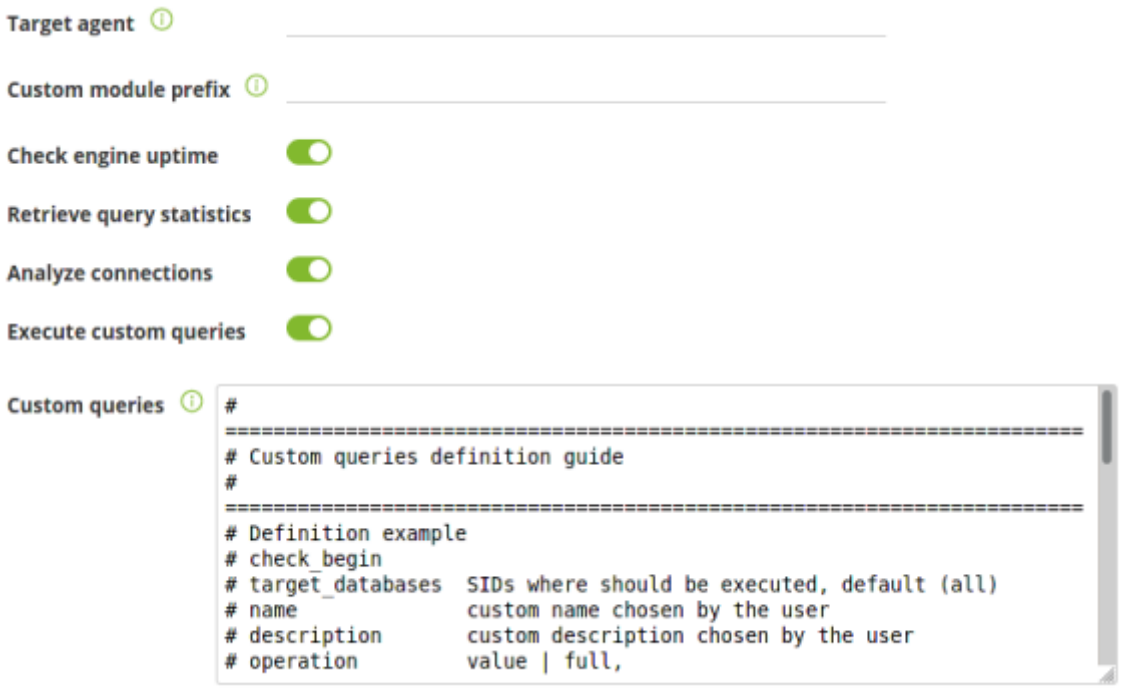
Чтобы определить порт:

```
IP:Puerto\Instancia
```

Пример:

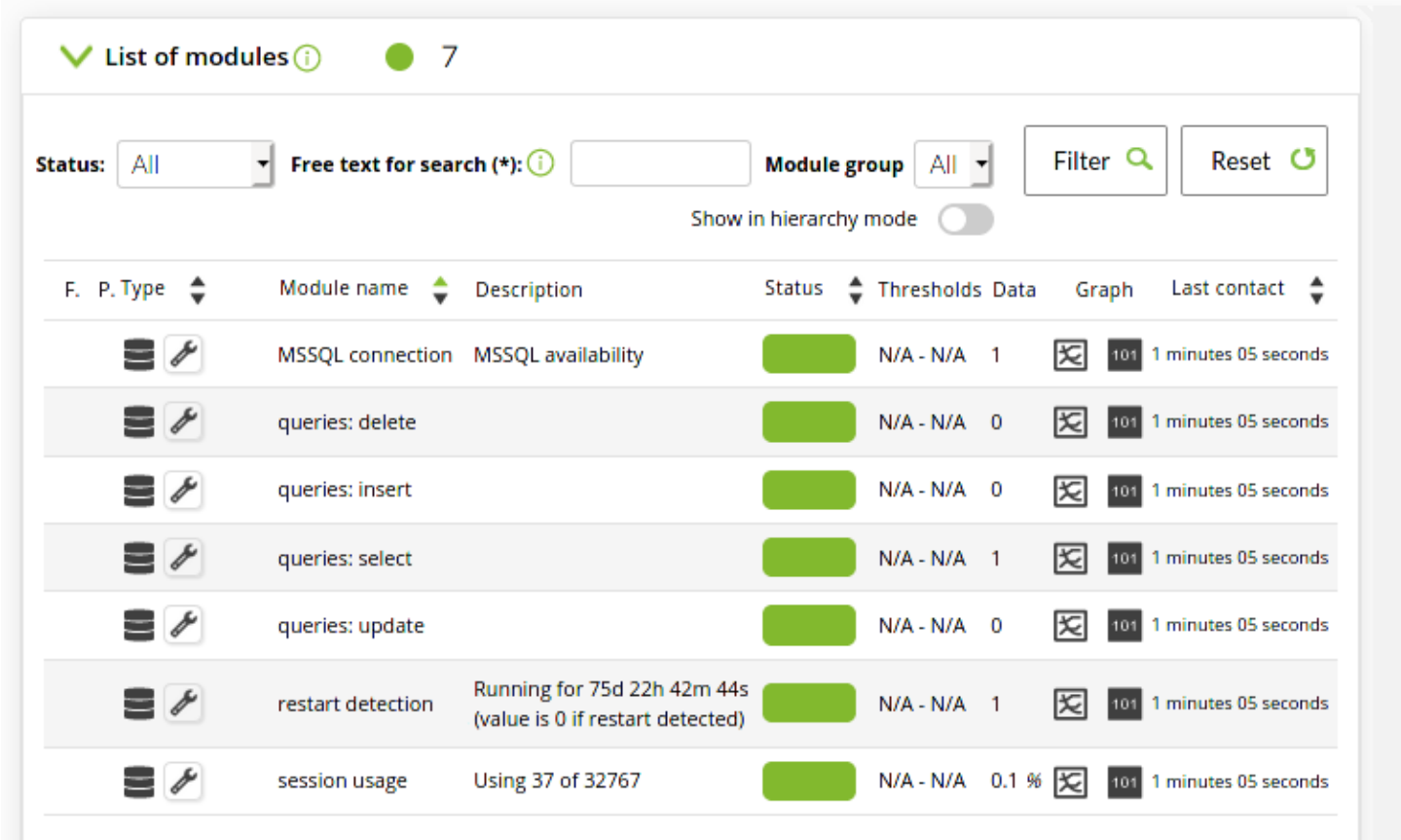


Расширенные параметры конфигурации для этой интеграции включают стабильность сервиса, статистику использования, статус соединения и пользовательские запросы.



Чтобы запустить пользовательский запрос, вы должны настроить его таким же образом, как и задачи Oracle®, как показано выше.

Модули, доступные по умолчанию



Пользователь и учетные данные, используемые для мониторинга, должны иметь

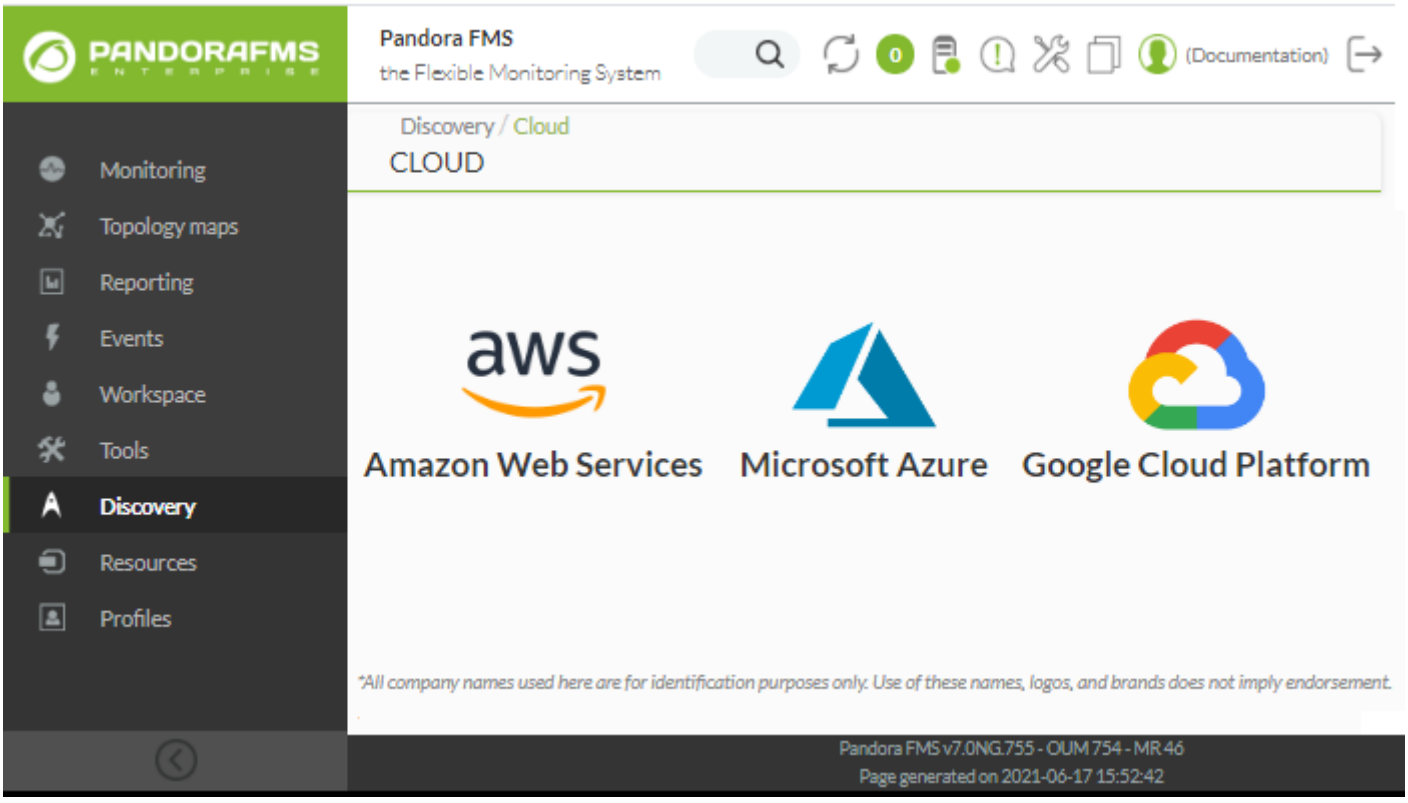
необходимые разрешения на подключаемые базы данных для выполнения соответствующих операций.

Nombre	Descripción
MSSQL connection	Проверяет, есть ли соединение с сервером MS SQL.
queries: delete	Количество запросов на удаление, выполненных с момента последней проверки.
queries: insert	Количество запросов на вставку, выполненных с момента последней проверки.
queries: update	Количество запросов на обновление, выполненных с момента последней проверки.
queries: select	Количество запросов на чтение, выполненных с момента последней проверки.
restart detection	Проверяет, как долго служба базы данных работает непрерывно.
session usage	Процент открытых сессий по отношению к максимально доступным. Отображает текущее и максимальное значение в описании модуля.

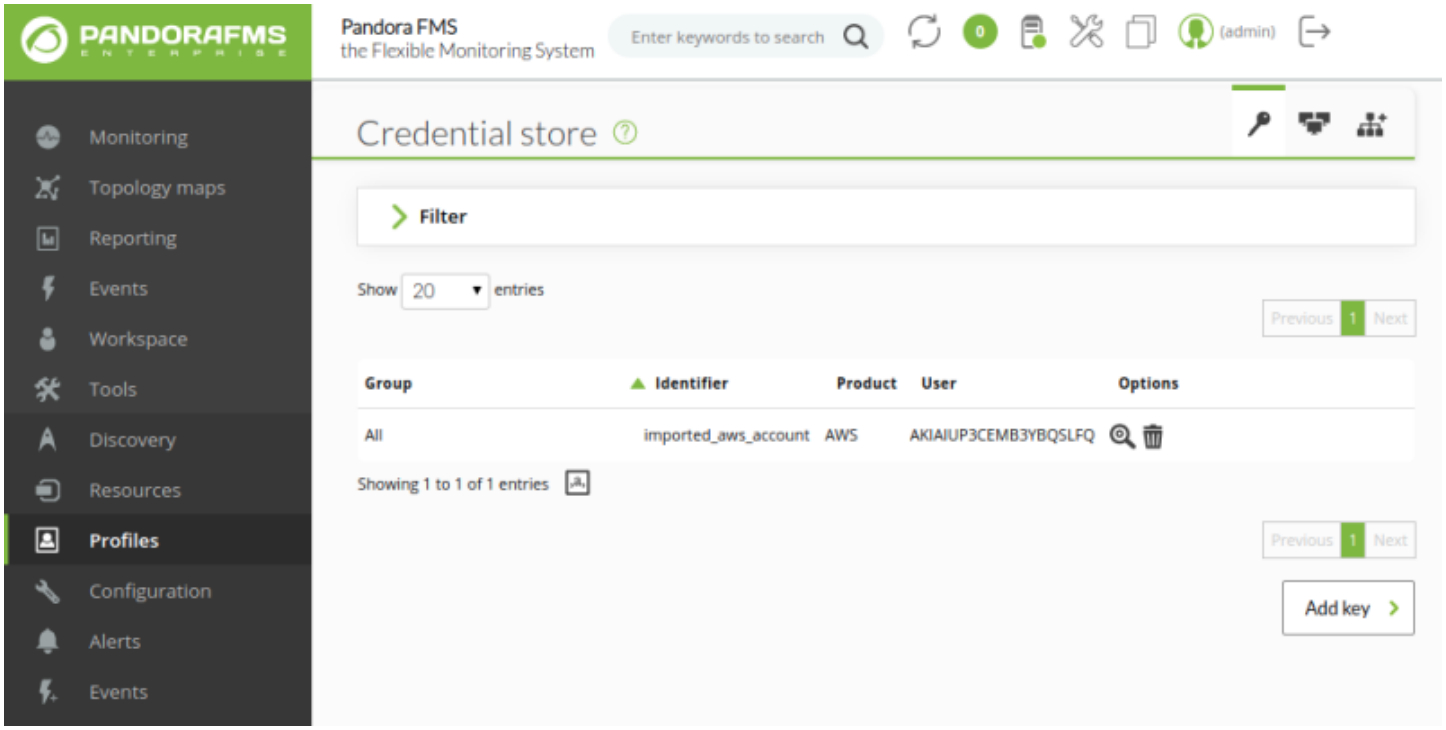
Discovery Cloud

Вернуться наверх ♦

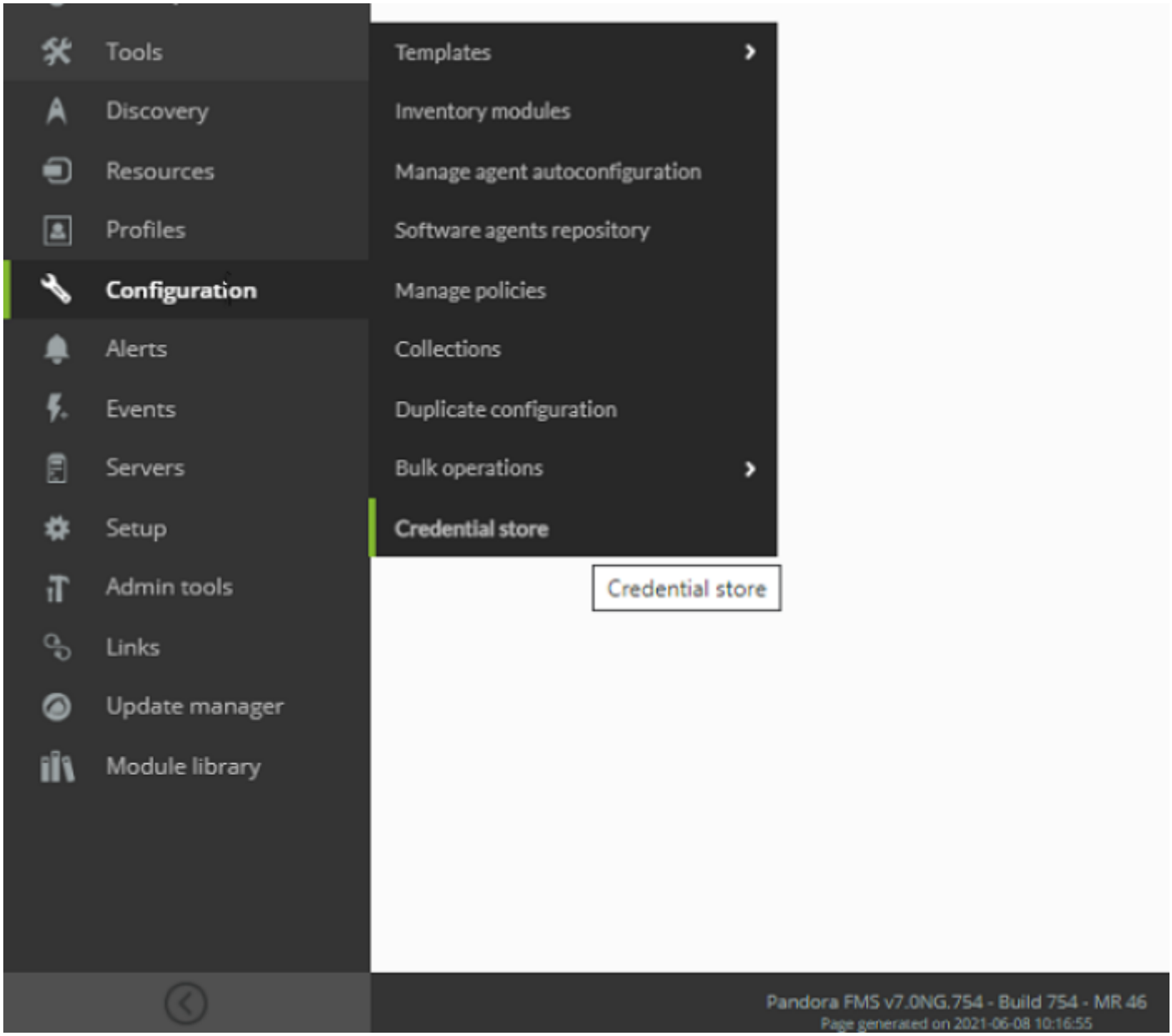
Discovery Cloud позволяет отслеживать учетные записи Amazon Web Services®, Google Cloud Platform®, а также Microsoft Azure® в одном инструменте.



Управление всеми учетными записями осуществляется через Credential Store, расположенный в Profiles → Manage agent groups → Credential Store.



Начиная с версии NG 754 и далее, используйте меню;
Configuration → Credential store



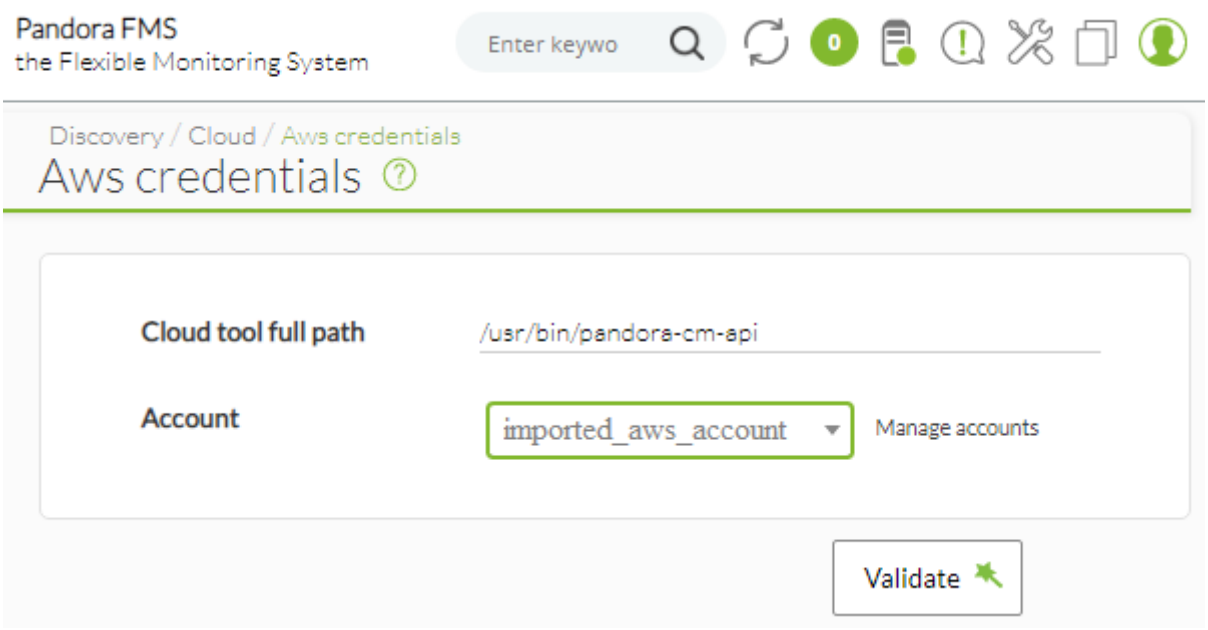
Discovery Cloud: Amazon Web Services (AWS)

Этот раздел находится в стадии разработки.

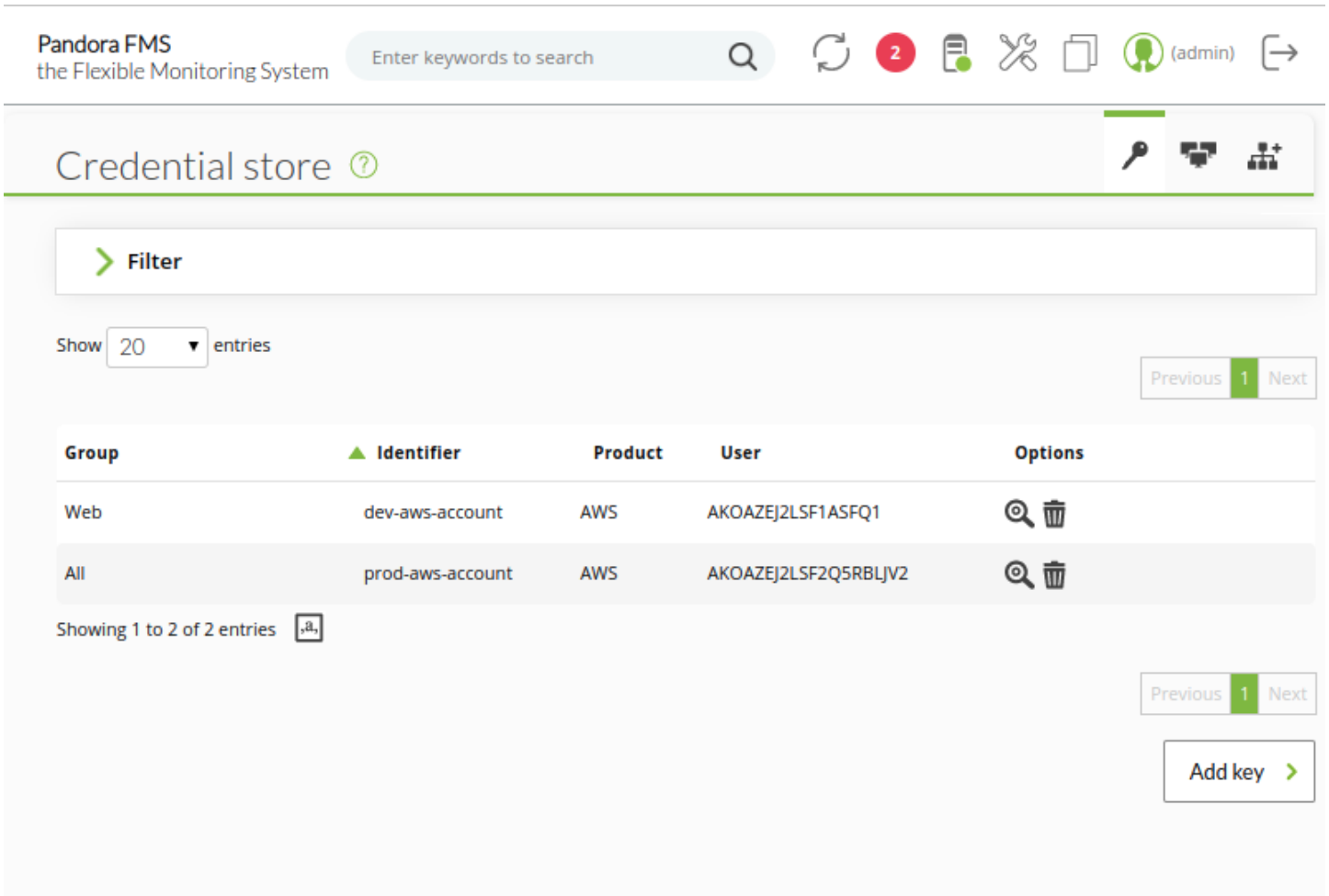
Для мониторинга инфраструктуры в Amazon Web Services необходимо шаг за шагом пройти различные страницы помощника.

Подтверждение полномочий AWS

При входе в меню Amazon Web Services® вам будет предложено выбрать учетную запись AWS; если она зарегистрирована в предыдущих версиях, она будет отображаться как imported_aws_account.

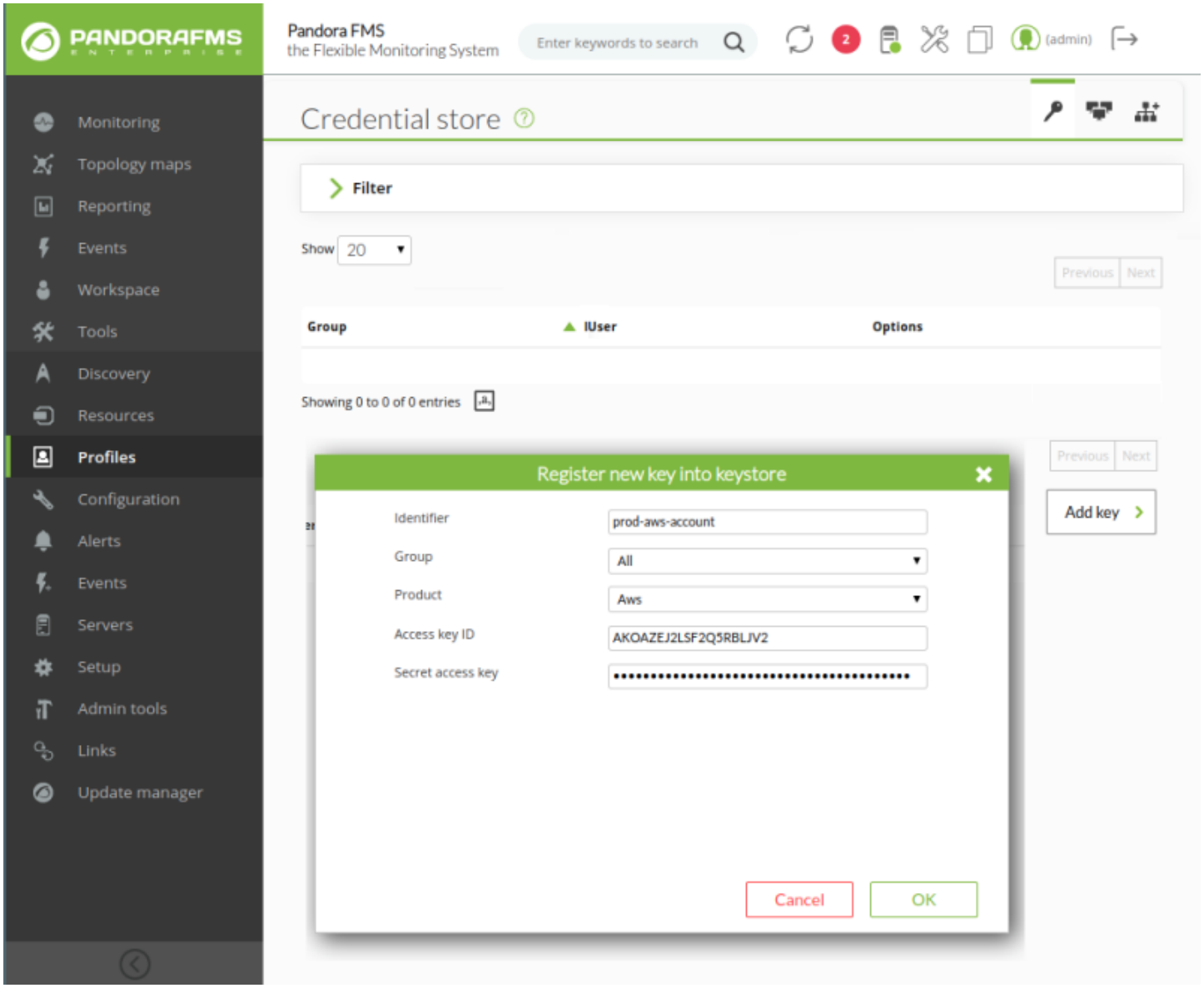


Для добавления дополнительных учетных записей используйте опцию Manage Accounts, расположенную рядом с выпадающим меню AWS Account. Затем в разделе Credential store раздела Profiles > Manage agent groups сохраните все ранее созданные учетные записи Amazon Web Services.

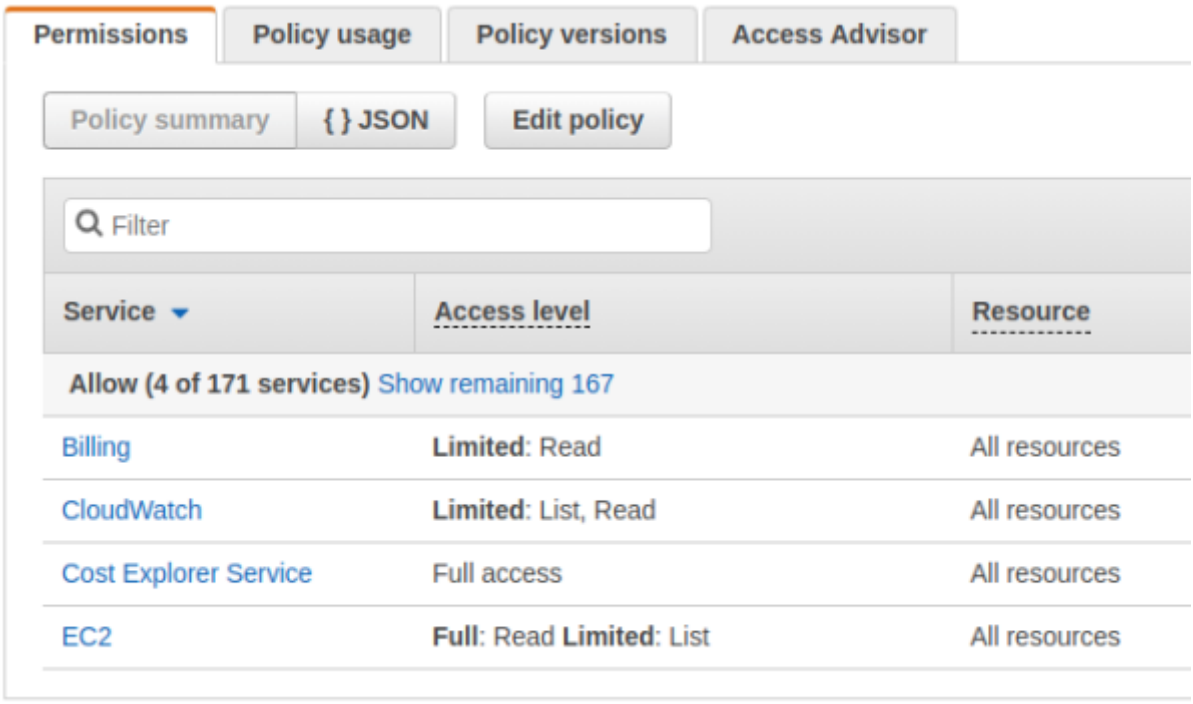


Для каждой учетной записи в хранилище учетных

данных можно выполнить только одну задачу в Amazon EC2 Discovery.



Вы должны перейти в AWS и создать учетные записи запросов со следующими разрешениями:



- Billing (read)
- CloudWatch (list,read)
- Cost Explorer Service (Full access)
- EC2 (full read, limited: list)

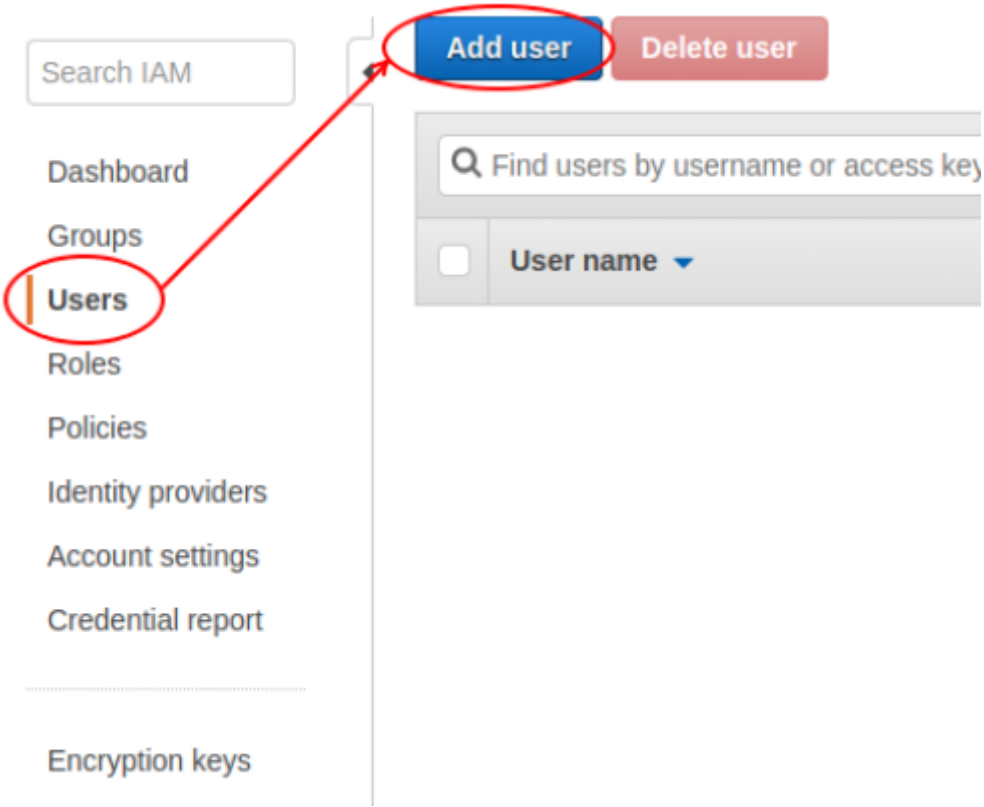
Сводка политики в формате JSON:

```
{
   "Version": "2012-10-17",
   "Statement": [
       {
           "Sid": "VisualEditor0",
           "Effect": "Allow",
           "Action": [
               "ec2:DescribeInstances",
               "ec2:DescribeVolumesModifications",
               "ec2:GetHostReservationPurchasePreview",
               "ec2:DescribeSnapshots",
               "aws-portal:ViewUsage",
               "ec2:DescribePlacementGroups",
               "ec2:GetConsoleScreenshot",
               "ec2:DescribeHostReservationOfferings",
               "ec2:DescribeInternetGateways",
               "ec2:GetLaunchTemplateData",
               "ec2:DescribeVolumeStatus",
               "ec2:DescribeScheduledInstanceAvailability",
               "ec2:DescribeSpotDatafeedSubscription",
               "ec2:DescribeVolumes",
               "ec2:DescribeFpgaImageAttribute",
               "ec2:DescribeExportTasks",
               "ec2:DescribeAccountAttributes",
               "aws-portal:ViewBilling",
```

```
                "ec2:DescribeNetworkInterfacePermissions",
                "ec2:DescribeReservedInstances",
                "ec2:DescribeKeyPairs",
                "ec2:DescribeNetworkAcls",
                "ec2:DescribeRouteTables",
                "ec2:DescribeReservedInstancesListings",
                "ec2:DescribeEgressOnlyInternetGateways",
                "ec2:DescribeSpotFleetRequestHistory",
                "ec2:DescribeLaunchTemplates",
                "ec2:DescribeVpcClassicLinkDnsSupport",
                "ec2:DescribeVpnConnections",
                "ec2:DescribeSnapshotAttribute",
                "ec2:DescribeVpcPeeringConnections",
                "ec2:DescribeReservedInstancesOfferings",
                "ec2:DescribeIdFormat",
                "ec2:DescribeVpcEndpointServiceConfigurations",
                "ec2:DescribePrefixLists",
                "cloudwatch:GetMetricStatistics",
                "ec2:GetReservedInstancesExchangeQuote",
                "ec2:DescribeVolumeAttribute",
                "ec2:DescribeInstanceCreditSpecifications",
                "ec2:DescribeVpcClassicLink",
                "ec2:DescribeImportSnapshotTasks",
                "ec2:DescribeVpcEndpointServicePermissions",
                "ec2:GetPasswordData",
                "ec2:DescribeScheduledInstances",
                "ec2:DescribeImageAttribute",
                "ec2:DescribeVpcEndpoints",
                "ec2:DescribeReservedInstancesModifications",
                "ec2:DescribeElasticGpus",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpnGateways",
                "ec2:DescribeMovingAddresses",
                "ec2:DescribeAddresses",
                "ec2:DescribeInstanceAttribute",
                "ec2:DescribeRegions",
                "ec2:DescribeFlowLogs",
                "ec2:DescribeDhcpOptions",
                "ec2:DescribeVpcEndpointServices",
                "ce:GetCostAndUsage",
                "ec2:DescribeSpotInstanceRequests",
                "cloudwatch:ListMetrics",
                "ec2:DescribeVpcAttribute",
                "ec2:GetConsoleOutput",
                "ec2:DescribeSpotPriceHistory",
                "ce:GetReservationUtilization",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeNetworkInterfaceAttribute",
                "ce:GetDimensionValues",
                "ec2:DescribeVpcEndpointConnections",
                "ec2:DescribeInstanceStatus",
```

```
                "ec2:DescribeHostReservations",
                "ec2:DescribeIamInstanceProfileAssociations",
                "ec2:DescribeTags",
                "ec2:DescribeLaunchTemplateVersions",
                "ec2:DescribeBundleTasks",
                "ec2:DescribeIdentityIdFormat",
                "ec2:DescribeImportImageTasks",
                "ec2:DescribeClassicLinkInstances",
                "ec2:DescribeNatGateways",
                "ec2:DescribeCustomerGateways",
                "ec2:DescribeVpcEndpointConnectionNotifications",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSpotFleetRequests",
                "ec2:DescribeHosts",
                "ec2:DescribeImages",
                "ec2:DescribeFpgaImages",
                "ec2:DescribeSpotFleetInstances",
                "ec2:DescribeSecurityGroupReferences",
                "ec2:DescribeVpcs",
                "ec2:DescribeConversionTasks",
                "ec2:DescribeStaleSecurityGroups",
                "ce:GetTags"
            ],
            "Resource": "*"
        }
    ]
}
```

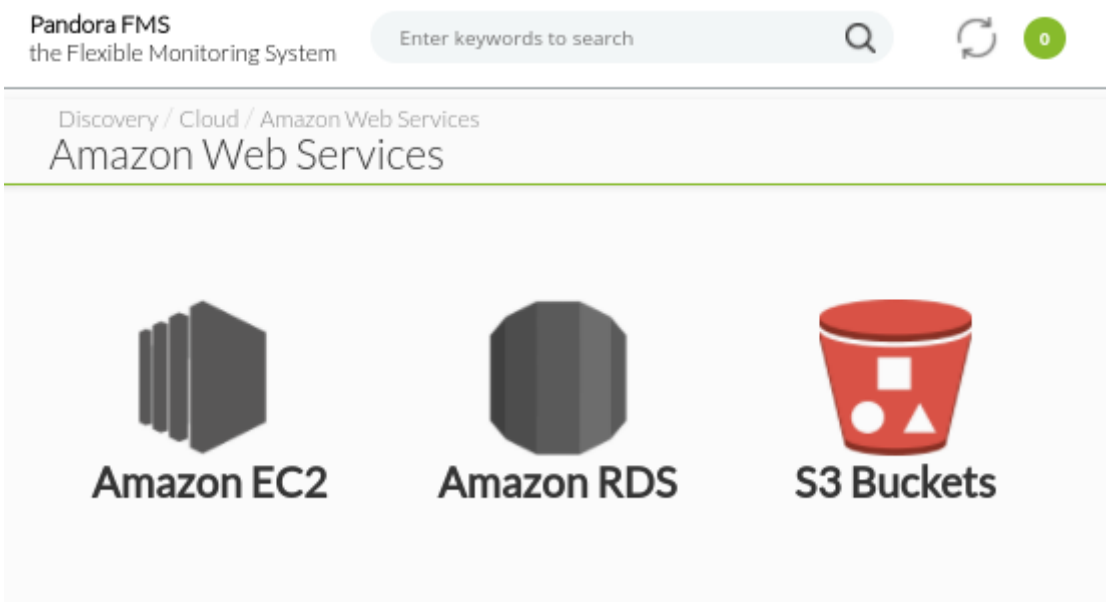
Приведенная выше политика должна быть назначена новому пользователю.



Когда вы вернетесь к конфигурации в Pandora FMS, вы сможете использовать зарегистрированную учетную запись для связи и доступа к мониторингу AWS.

Если в вашей установке нет pandora-cm-api, вы можете получить его по следующей ссылке: Pandora Cloud Monitoring API

Discovery Cloud AWS

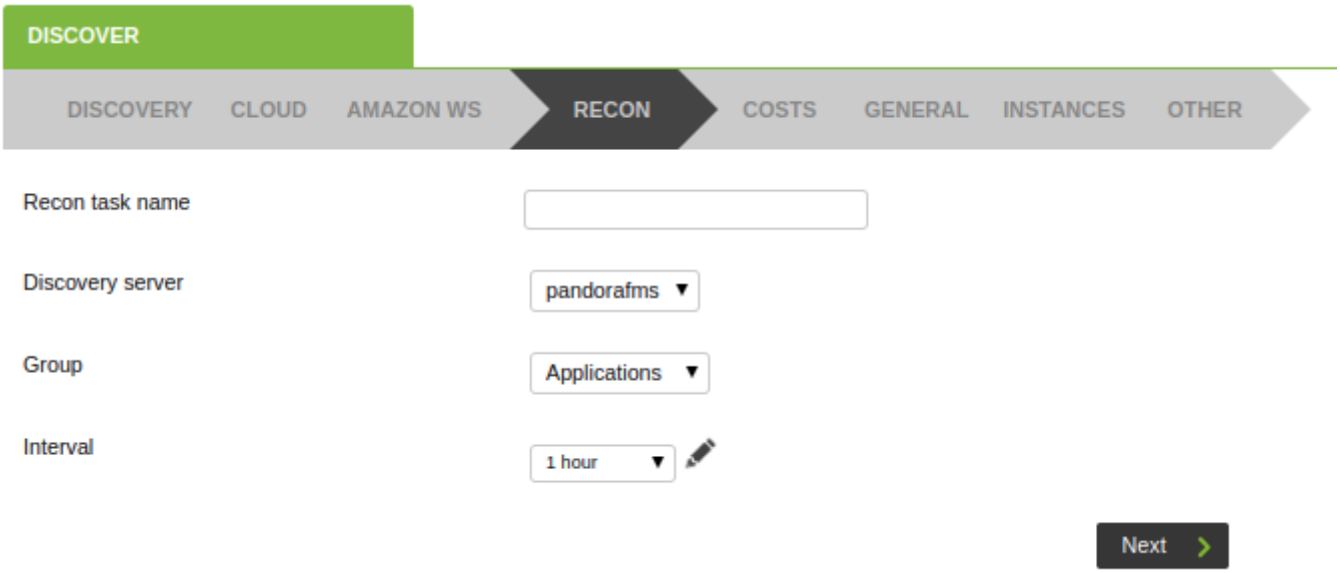


После подтверждения учетных данных необходимо войти в меню Discovery Cloud → Amazon Web Services. Для каждой учетной записи, добавленной в Credential store, можно контролировать среду EC2, размещенную на этой учетной записи.

Discovery Cloud AWS EC2

В рамках мониторинга EC2 доступна :

- Мониторинг затрат.
- Сводка ресурсов, зарегистрированных на AWS EC2.
- Мониторинг конкретных экземпляров.
- Мониторинг партий и статических IP-адресов.

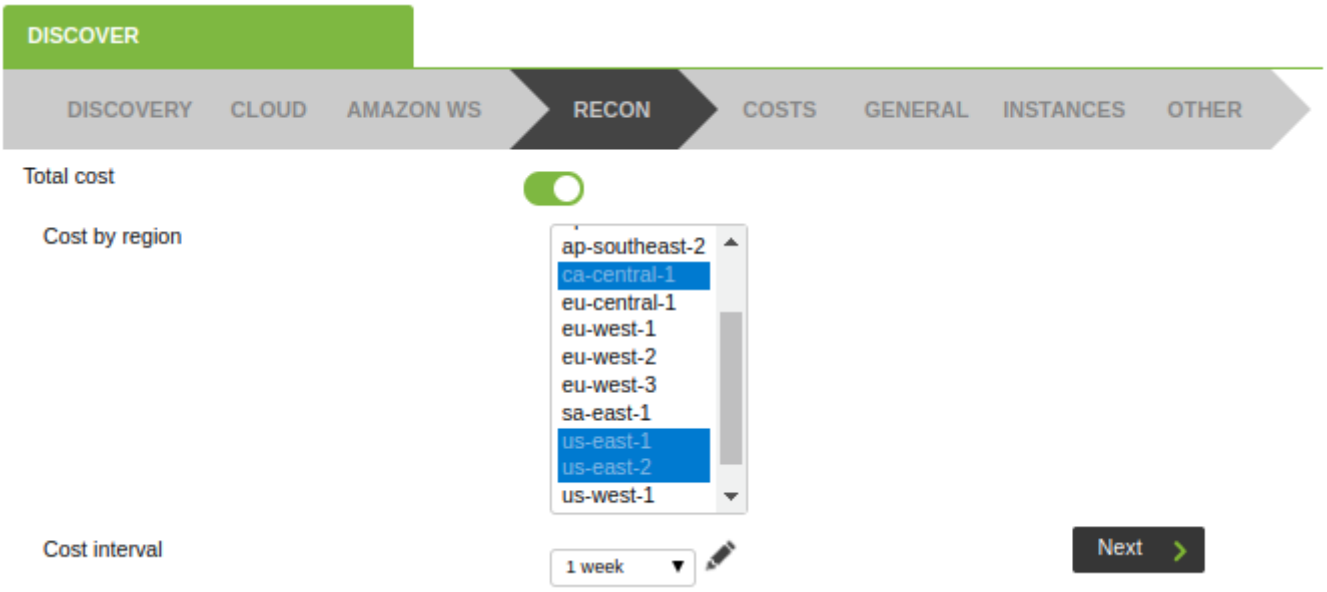


Чтобы начать процесс мониторинга, запрашивается ряд основных данных для задачи, таких как имя, сервер Discovery, который ее выполняет, группа и интервал.

Discovery Cloud Costes AWS EC2

Мониторинг стоимости Amazon Web Services предполагает дополнительные платежи, как объясняется здесь Amazon cost management pricing

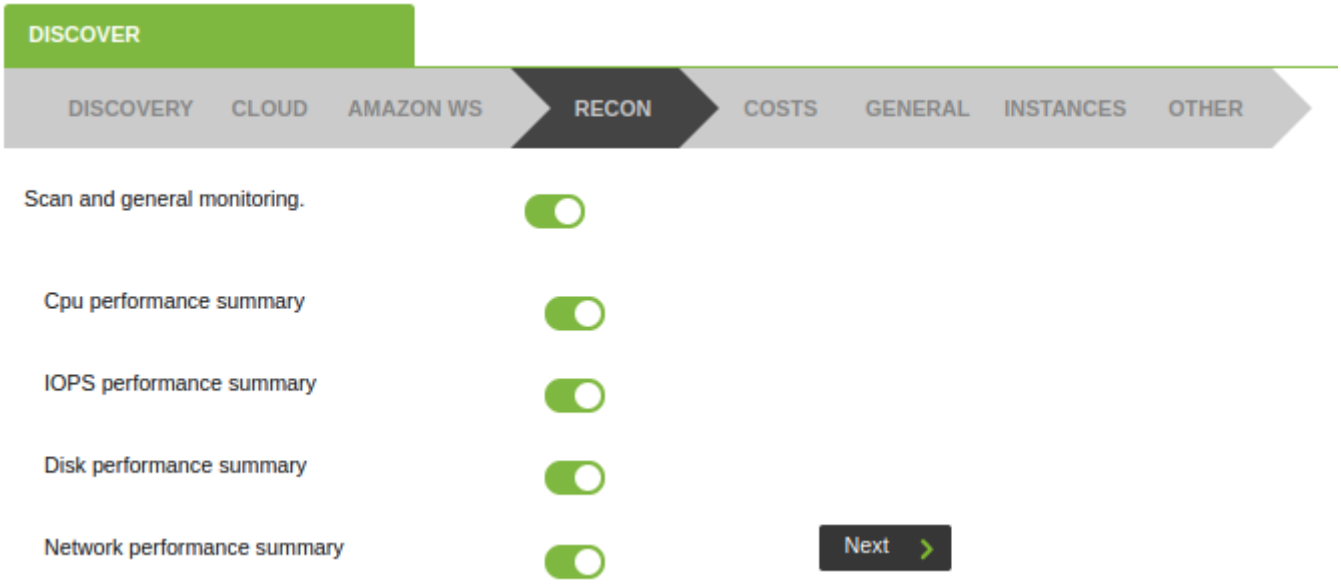
Мониторинг затрат обеспечивает независимый интервал мониторинга во избежание дополнительных расходов.



Вы можете контролировать как общие затраты, так и независимые затраты по областям.

Сводка Discovery Cloud AWS EC2

Вы можете настроить задачу на сбор общей информации о состоянии резерва во всех областях, включив опцию Scan and general monitoring.



Вы можете добавить общие счетчики для использования процессора, операций ввода-вывода (диск), объема переданных данных (байты) с диска и сети.

Мониторинг конкретных экземпляров AWS EC2

Конкретные экземпляры могут быть отслежены для получения показаний:

- CPUUtilization: Среднее использование процессора.
- DiskReadBytes: Байты считывания (диск).
- DiskWriteBytes: Байты записи (диск).
- DiskReadOps: Операции чтения (диск).
- DiskWriteOps: Операции записи (диск).
- NetworkPacketsIn: Входные пакеты (сеть).
- NetworkPacketsOut: Выходные пакеты (сеть).

Агенты, представляющие конкретные экземпляры, будут иметь в качестве родителя агента, представляющего область, в которой они размещены. *Токен* update_parent должен быть установлен в значение 1 на сервере Pandora FMS, чтобы поддерживать отношения родитель-ребенок в актуальном состоянии.

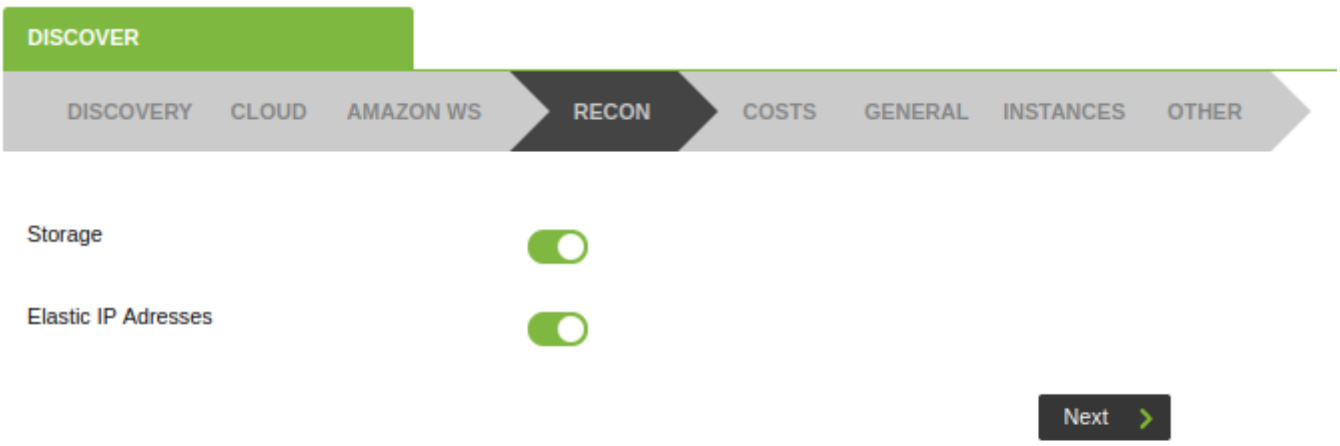
Вы должны перемещаться по проводнику, выбирая экземпляры, которые необходимо контролировать:

Discovery Cloud Extras AWS EC2

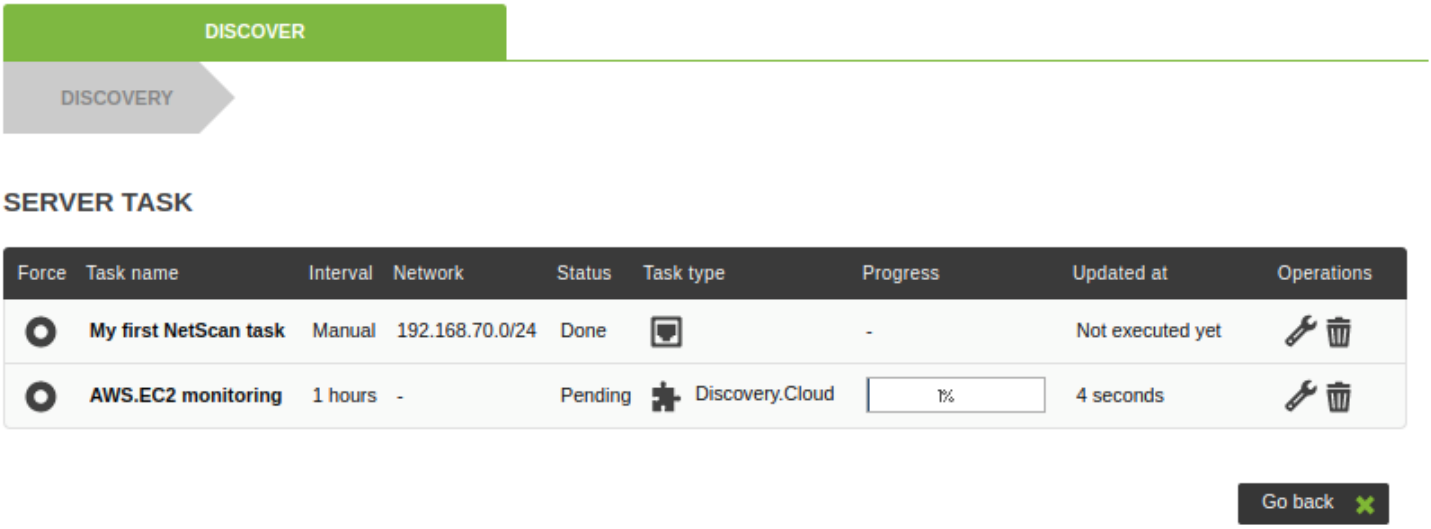
На этом последнем экране вы можете указать, хотите ли вы отслеживать партии, используемые зарезервированными экземплярами. В агентах области появятся два дополнительных модуля:

- Общий зарезервированный объем (ГБ).
- Всего зарегистрированных партий (количество).

Вы также можете включить *токен* Elastic IP Addresses, чтобы сообщить о количестве статических IP-адресов, зарегистрированных в вашей учетной записи AWS EC2.



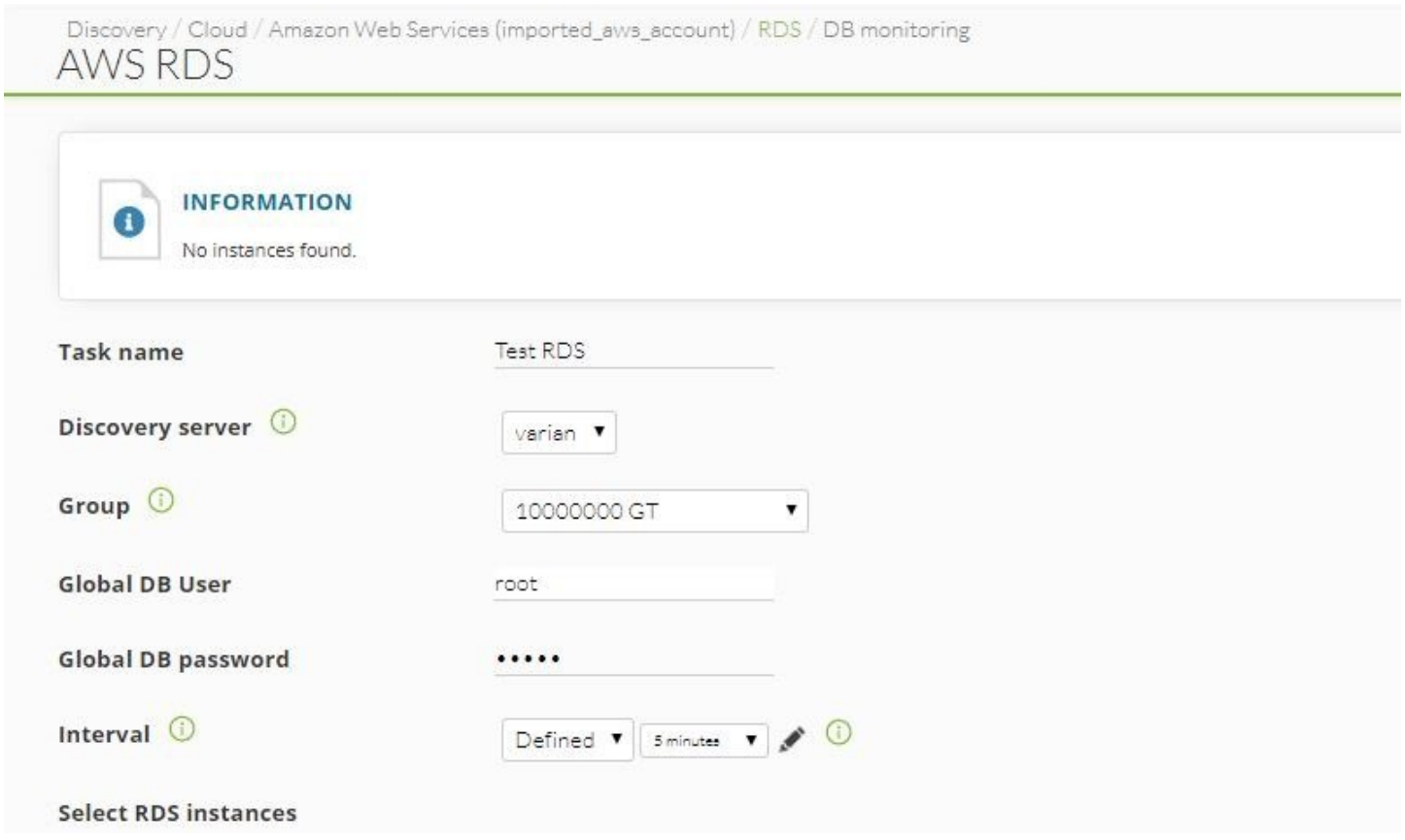
После завершения работы помощника вы можете просмотреть ход выполнения по адресу *Discovery Task list*:



Discovery Cloud AWS RDS

Служба RDS предоставляет сервер базы данных и позволяет создать экземпляр, связанный с этой базой данных. Он предлагает возможность подключения ваших экземпляров через такие клиенты, как SSMS, MySQL workbench или через JDBC или ODBC DB API.

Интеграция с AWS RDS поддерживает только Oracle,
MySQL и Mariadb.



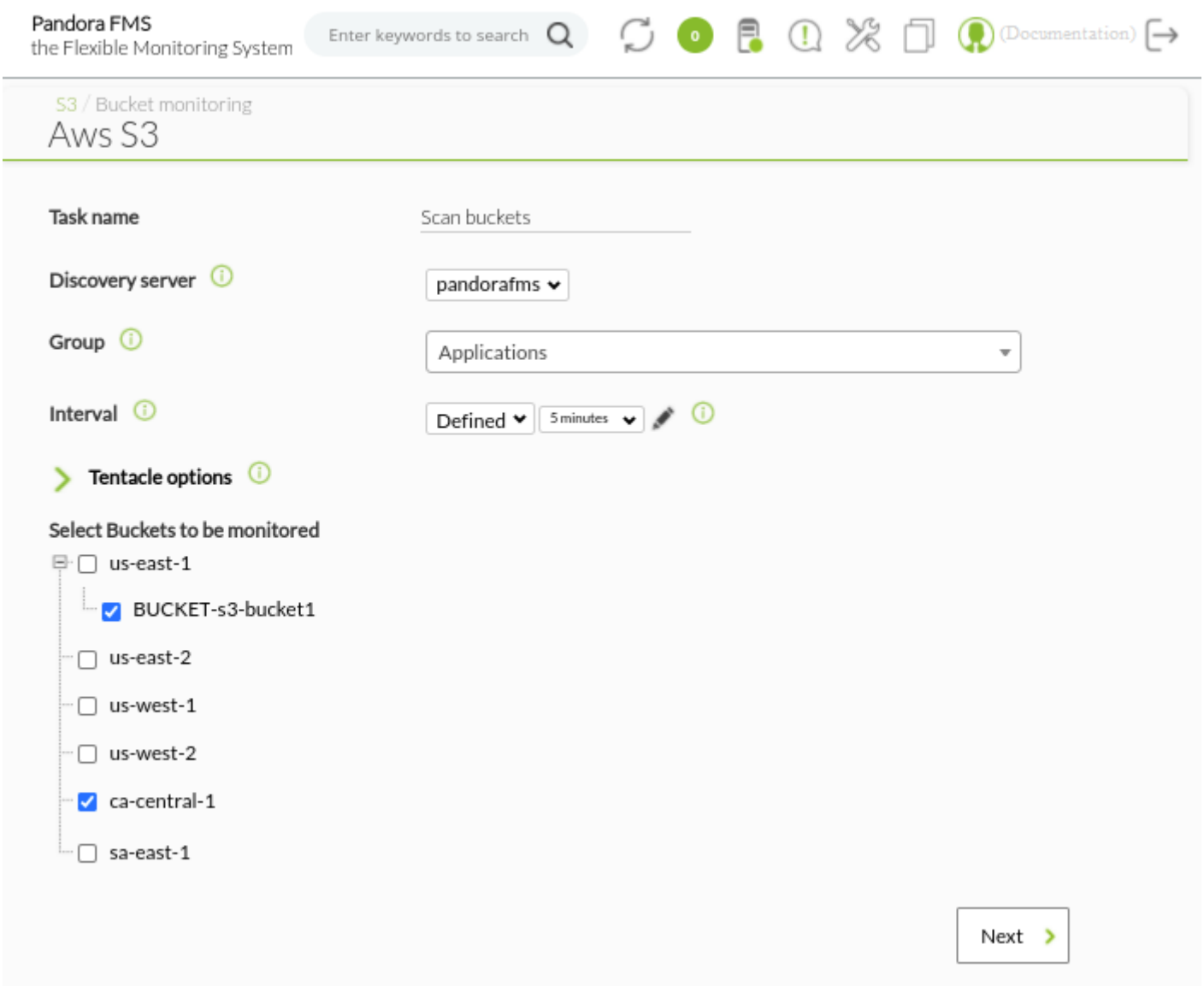
После выполнения предыдущих параметров можно отслеживать различные экземпляры

RDS, как происхождение данных, так и их доступность, а также все остальные метрики, которые можно отслеживать в базе данных (под RDS) на регулярной основе.

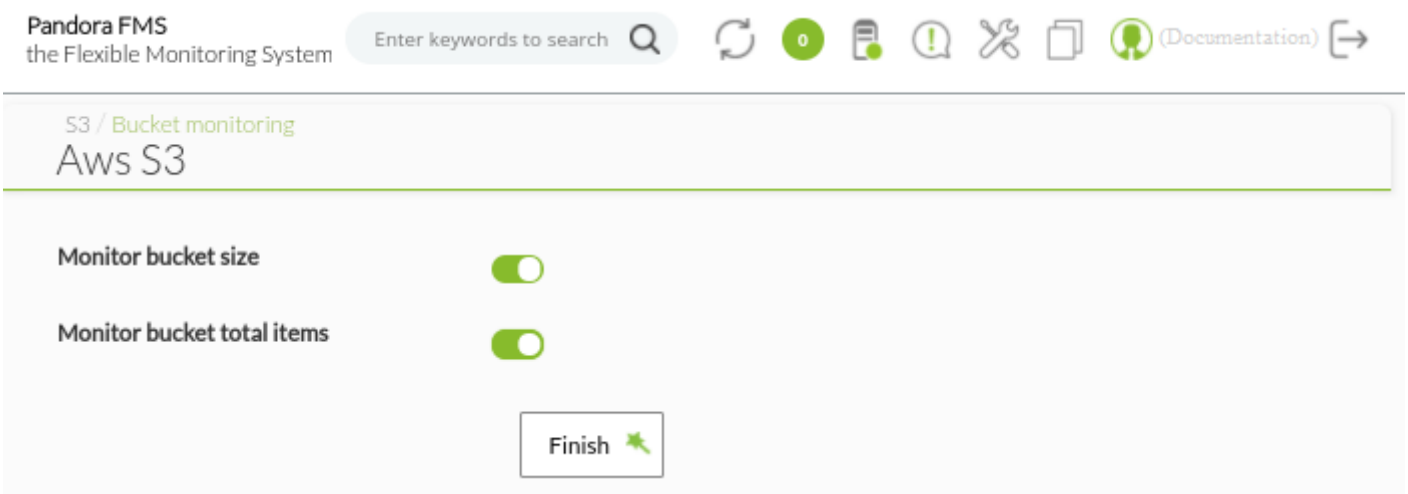
Discovery Cloud S3 Buckets

Служба S3 Buckets обеспечивает хранение файлов, называемых объектами, таких как корпоративные приложения, *data lakes* , мобильные приложения, процессы резервного копирования и восстановления, операции архивирования и многие другие.

С помощью зарегистрированных учетных данных откройте доступ к созданию задачи исследования и выберите объекты для мониторинга, либо по одному, либо по областям.



Нажмите кнопку Next, чтобы перейти к следующему шагу: выберите размер Bucket и/или количество элементов в нем.



Сохраните изменения, нажав на Finish. Агенты, которые вы получите, будут глобальными AWS и контролируемыми областями; новыми модулями будут:

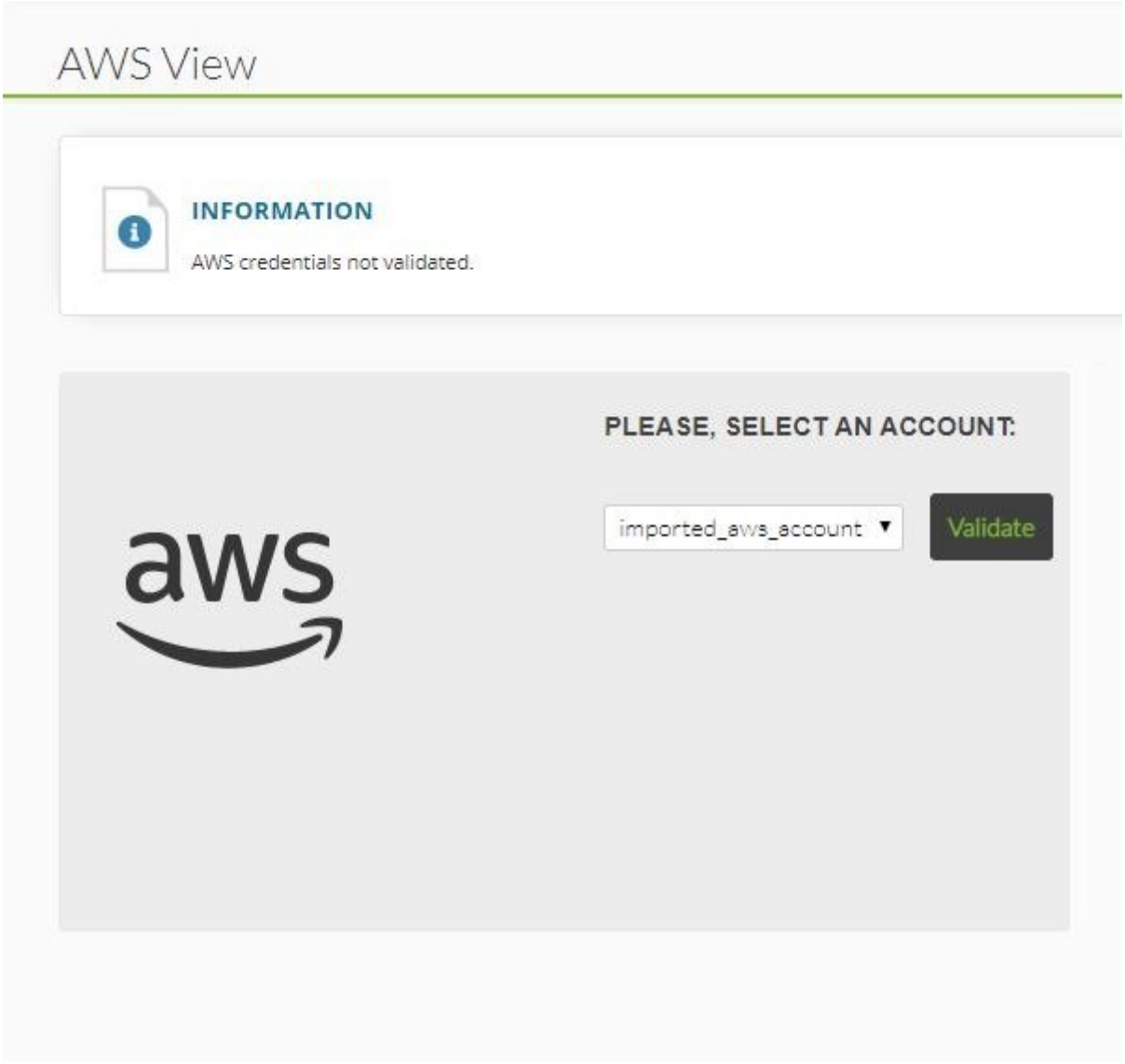
```
bucket.size <bucket-id> (region)
bucket.items <bucket-id> (region)
```

В случае мониторинга по областям, *bucket*, которое было обнаружено и отслежено, а затем удалено, оставит все его соответствующие модули в неизвестном состоянии. Unknown

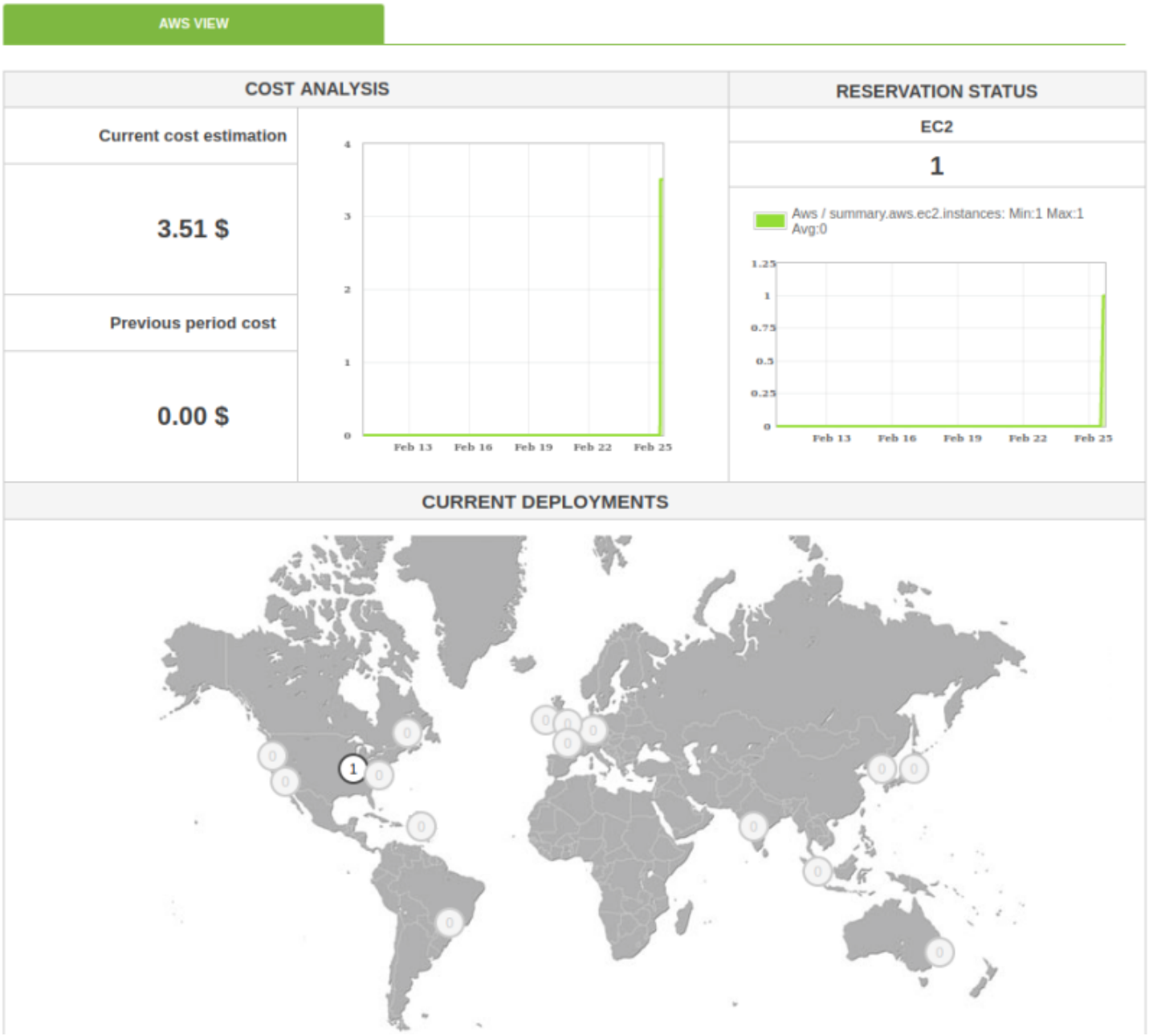
Discovery Cloud. Общий вид

Discovery Cloud включает обзор, в котором можно ознакомиться с ключевыми моментами инфраструктуры Amazon Web Services. Pandora FMS позволяет отображать различные карты в зависимости от существующих профилей.

При просмотре AWS вы можете выбрать профиль информации для отображения:



- Текущая стоимость
- Стоимость в предыдущем периоде
- График изменения затрат (6 месяцев)
- График эволюции бронирования/объектов (1 месяц)
- Карта областей с указанием количества экземпляров на область.

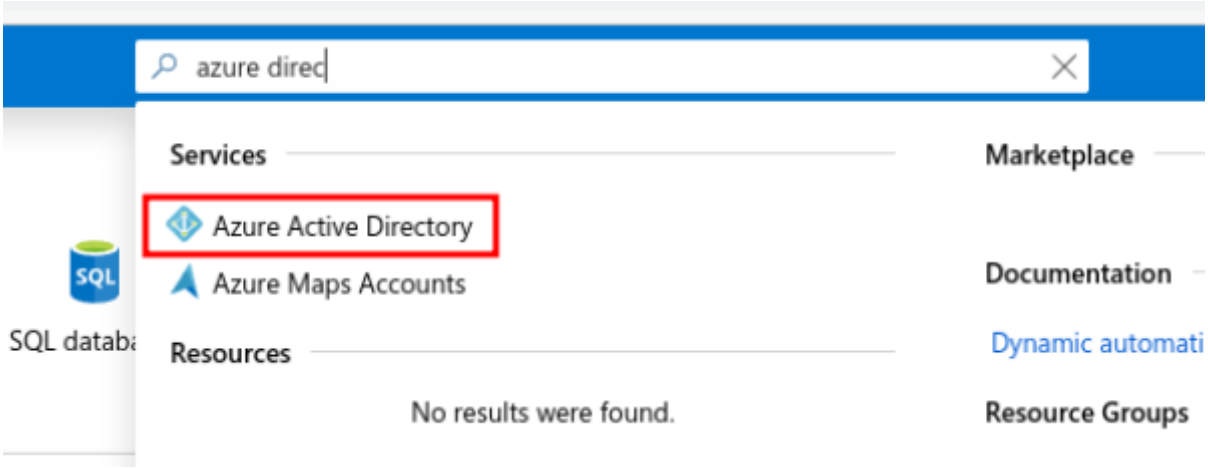


Discovery Cloud: Microsoft Azure

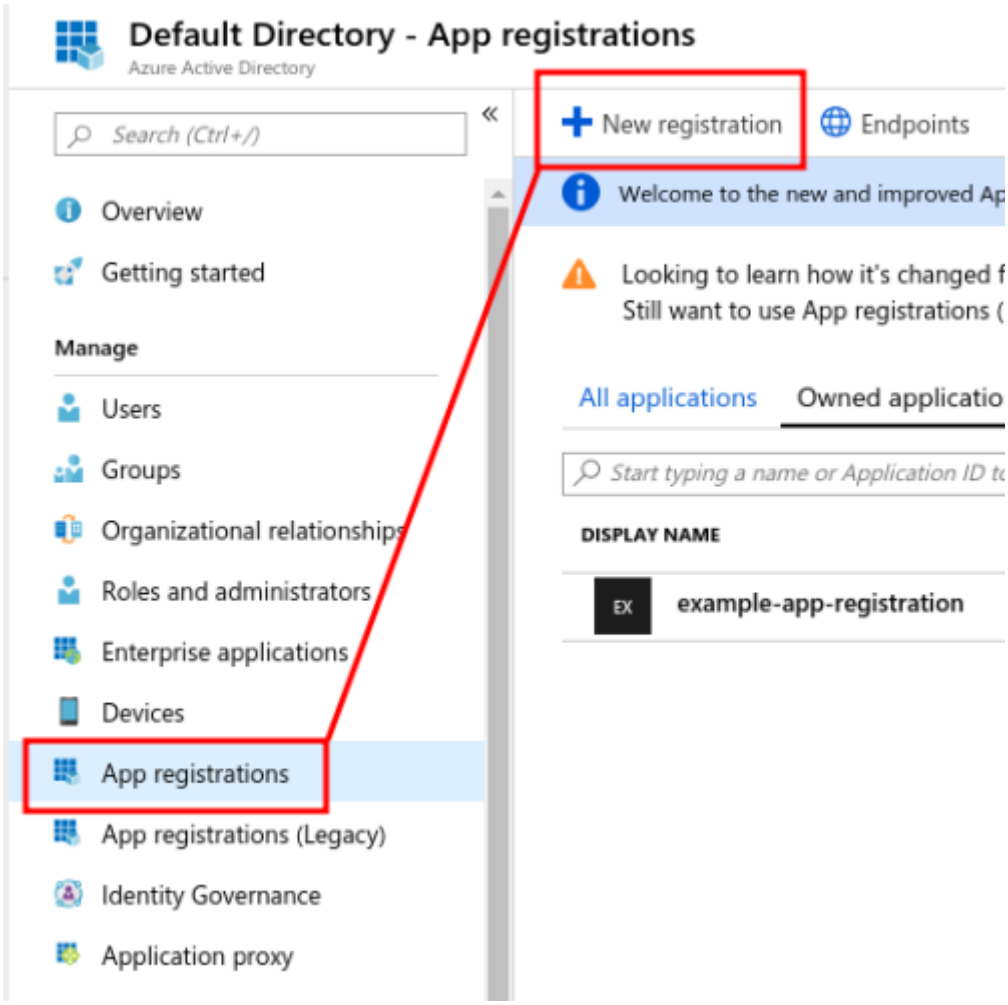
Для мониторинга инфраструктуры в Microsoft Azure® выполняйте шаг за шагом следующие инструкции.

Как зарегистрировать пользователя для использования Azure API?

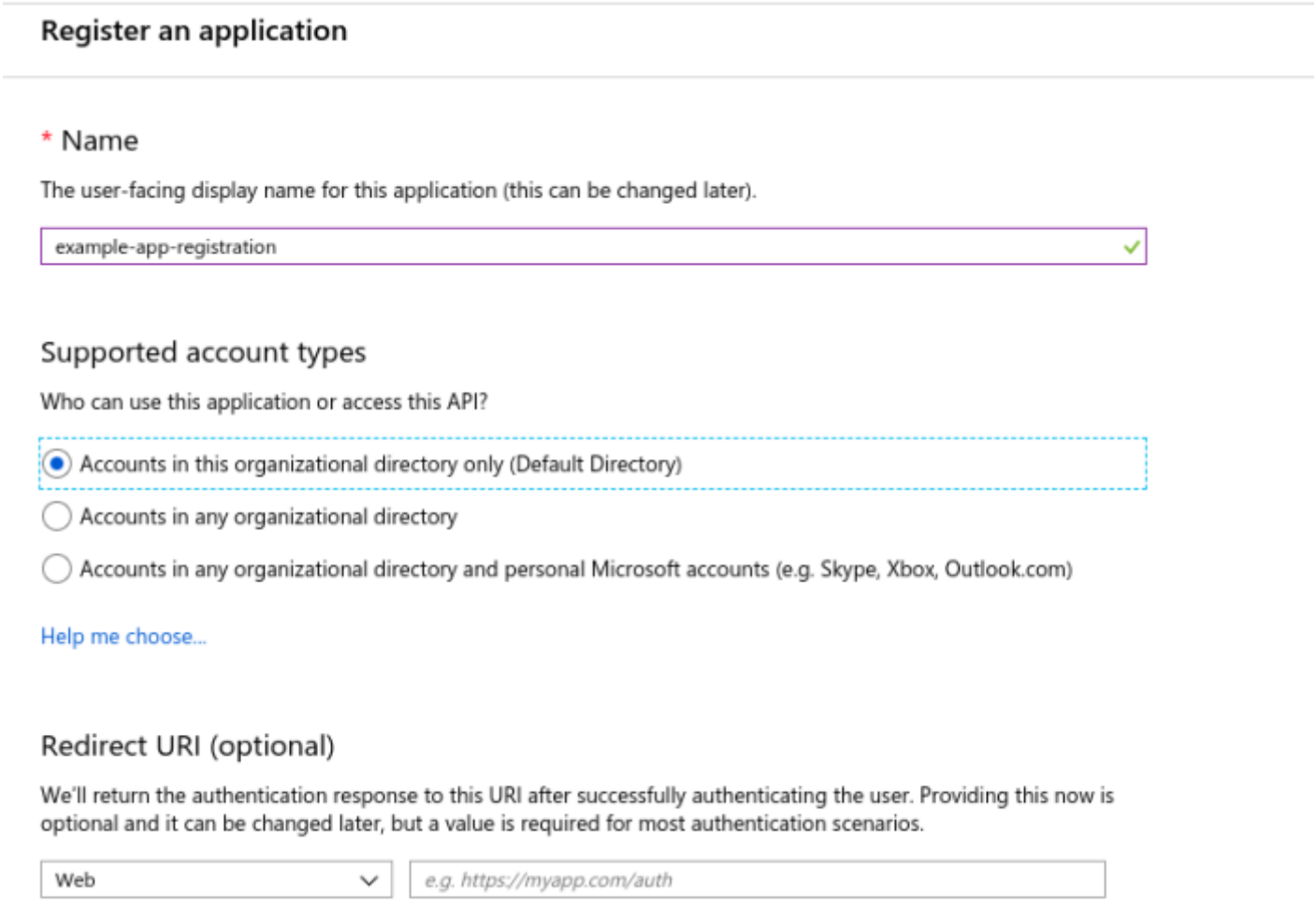
- Зайдите на портал Microsoft Azure®.
- Откройте сервис Azure Active Directory:



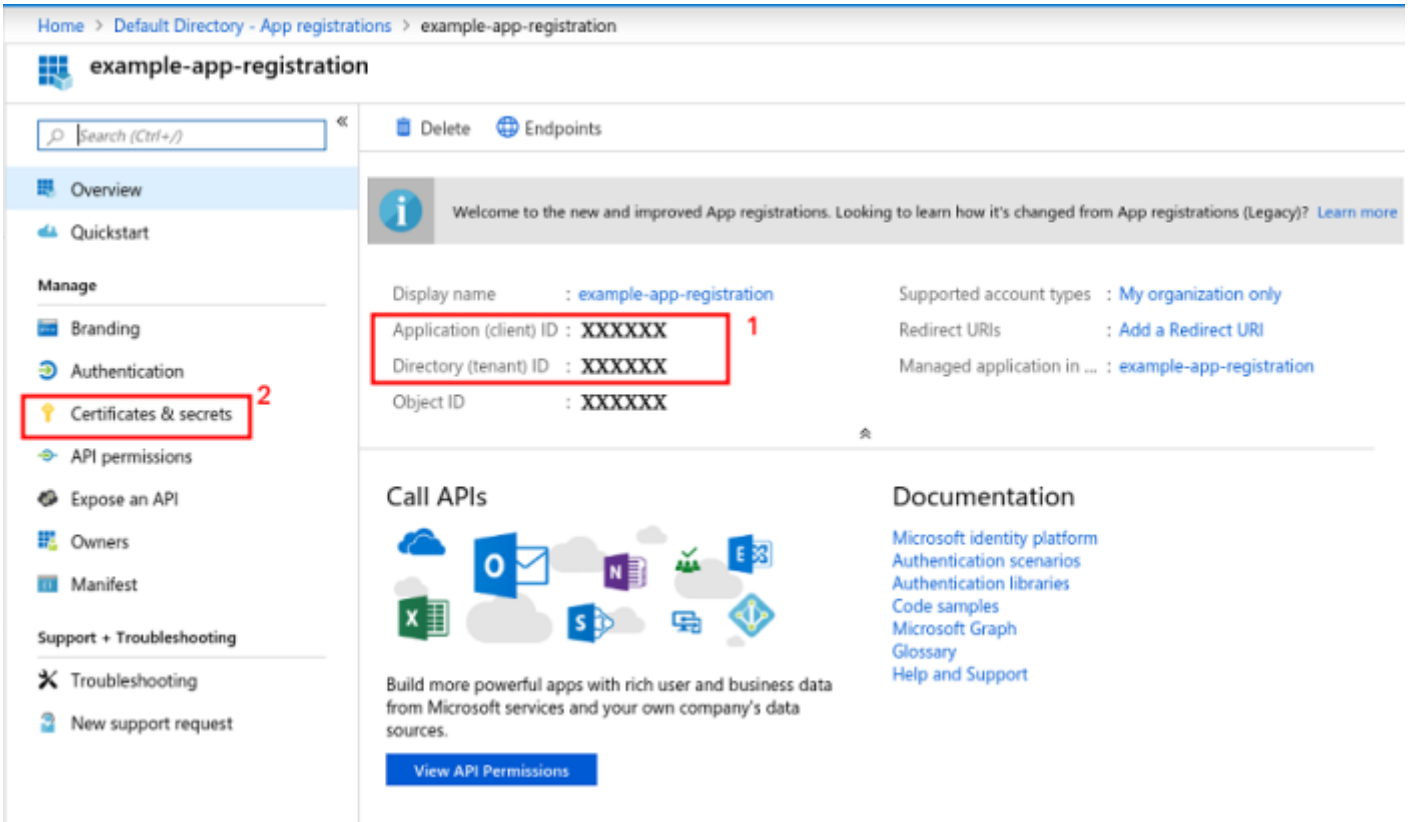
- Выберите App registrations > New registration:



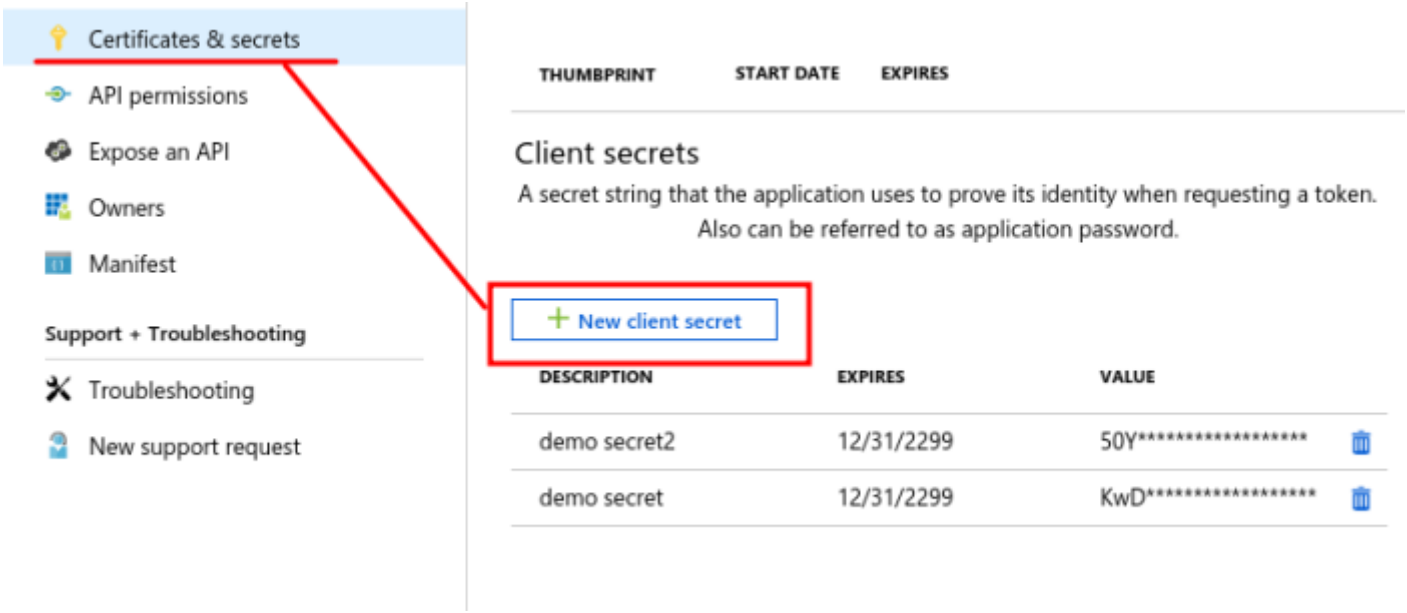
- Введите данные:



- Обратите особое внимание на значения Application (client) ID`client_id` и Directory (tenant) ID`directory>`



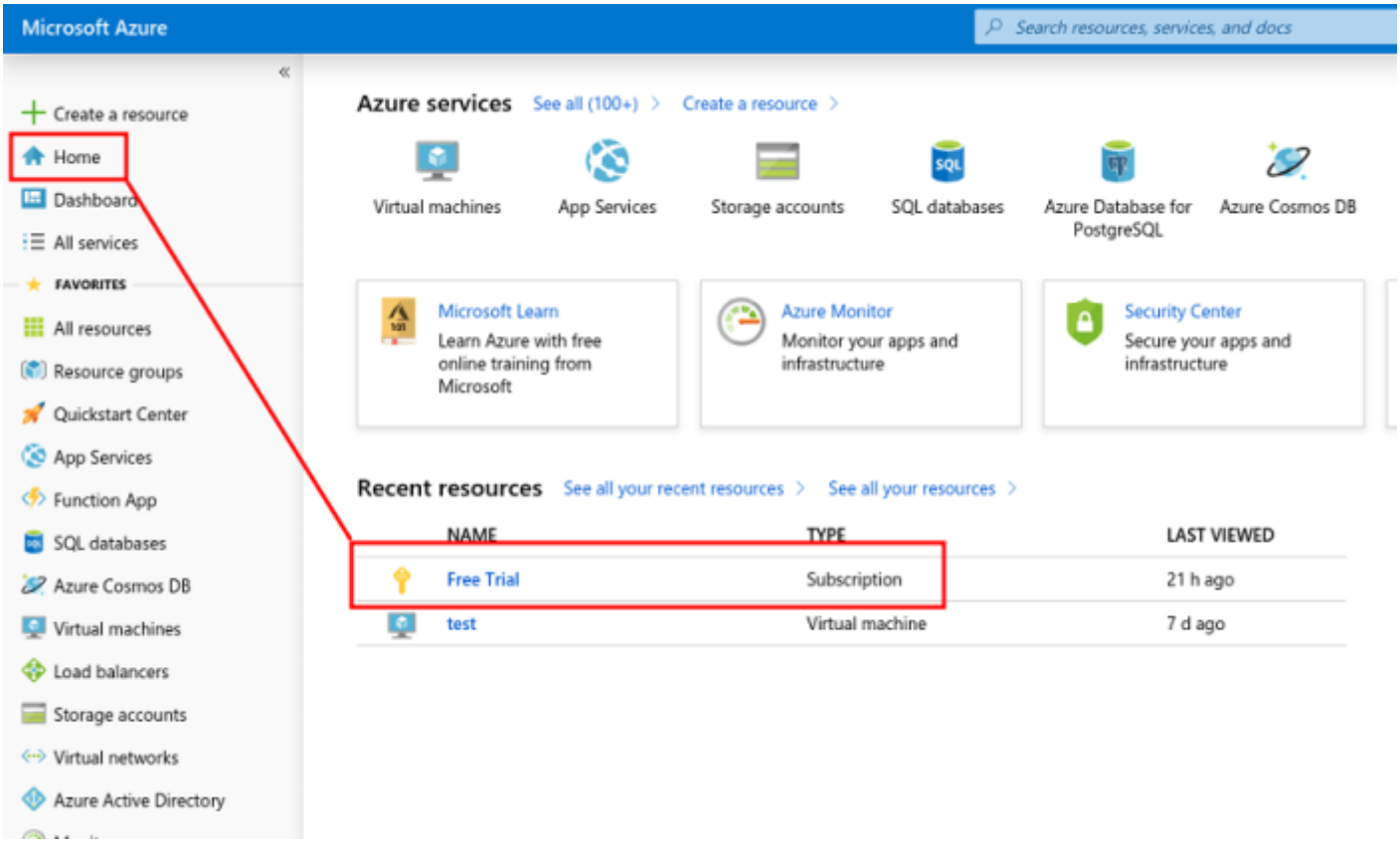
- Затем перейдите в раздел certificates & secrets и добавьте новый:



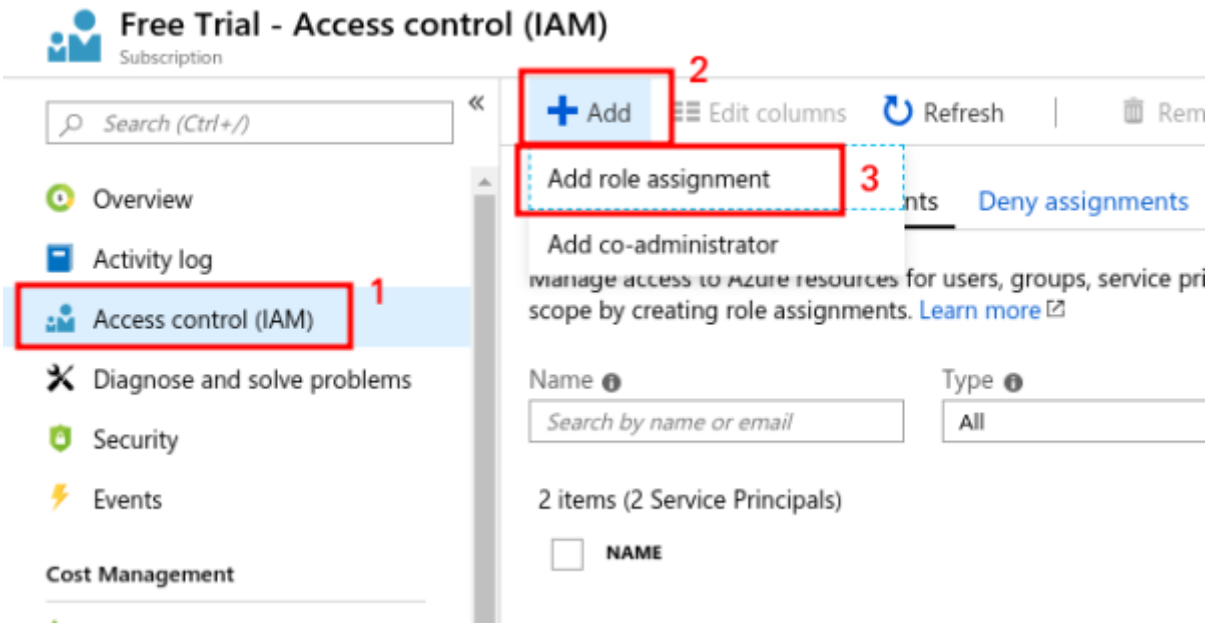
Необходимо записать пароль, который показан, этот пароль является `application_secret`.

Назначение разрешений

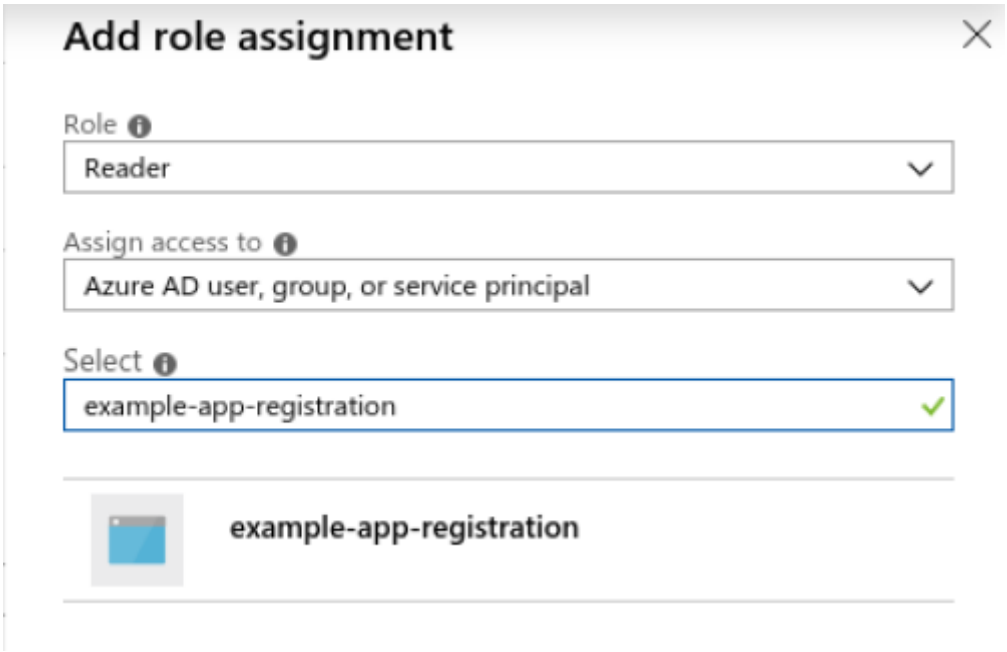
Вы должны назначить роль учетной записи, с которой будет работать *приложение*, для этого перейдите в Home и введите Subscription:



Внутри подписки выберите Access control (IAM):



Будет добавлено новое назначение роли, в котором вы должны выбрать Reader для созданного *приложения*:



Сохраните изменения, нажав *Save* .

С этого момента вы сможете подключаться к сервису и делать запросы через pandora-cm-api.

Примеры

Вы можете проверить статус MS Azure® из Pandora FMS:

- Предварительно загрузите среду.
- Выполните `. load_env.sh`

```
pandora-cm-api --product Azure --get availability.
```

Если среда работает, она возвращает значение 1.

Пример содержимого *скрипта* `load_env.sh>`

- Azure

```
export CLIENT_ID=XXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXX

 export DOMAIN=XXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXX

 export APPLICATION_SECRET="XXXXXXXXXXXXXXXXXXXXXXXXX"

 export AZURE_SUBSCRIPTION_ID=XXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXX
```

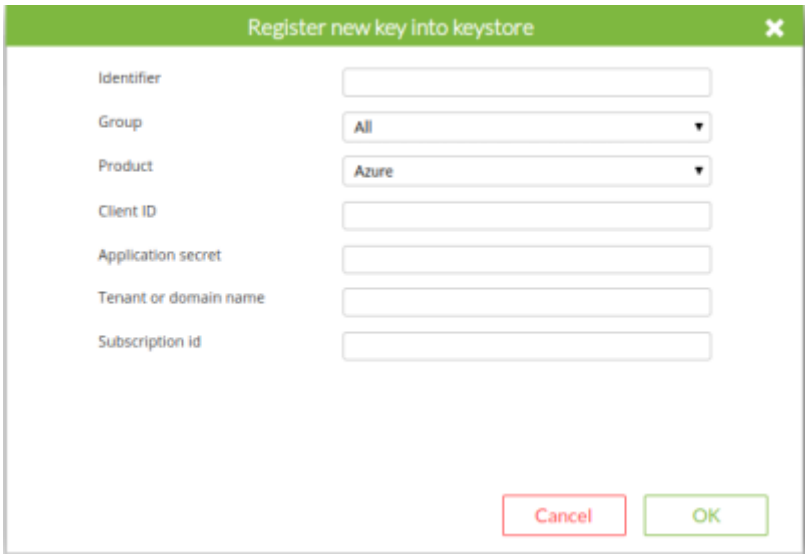
Настроить задачу в Pandora FMS

Pandora FMS позволяет управлять несколькими учетными записями Microsoft Azure®. Вы можете добавить столько учетных записей, сколько вам нужно, с помощью опции Manage Accounts рядом с выпадающим меню Account.

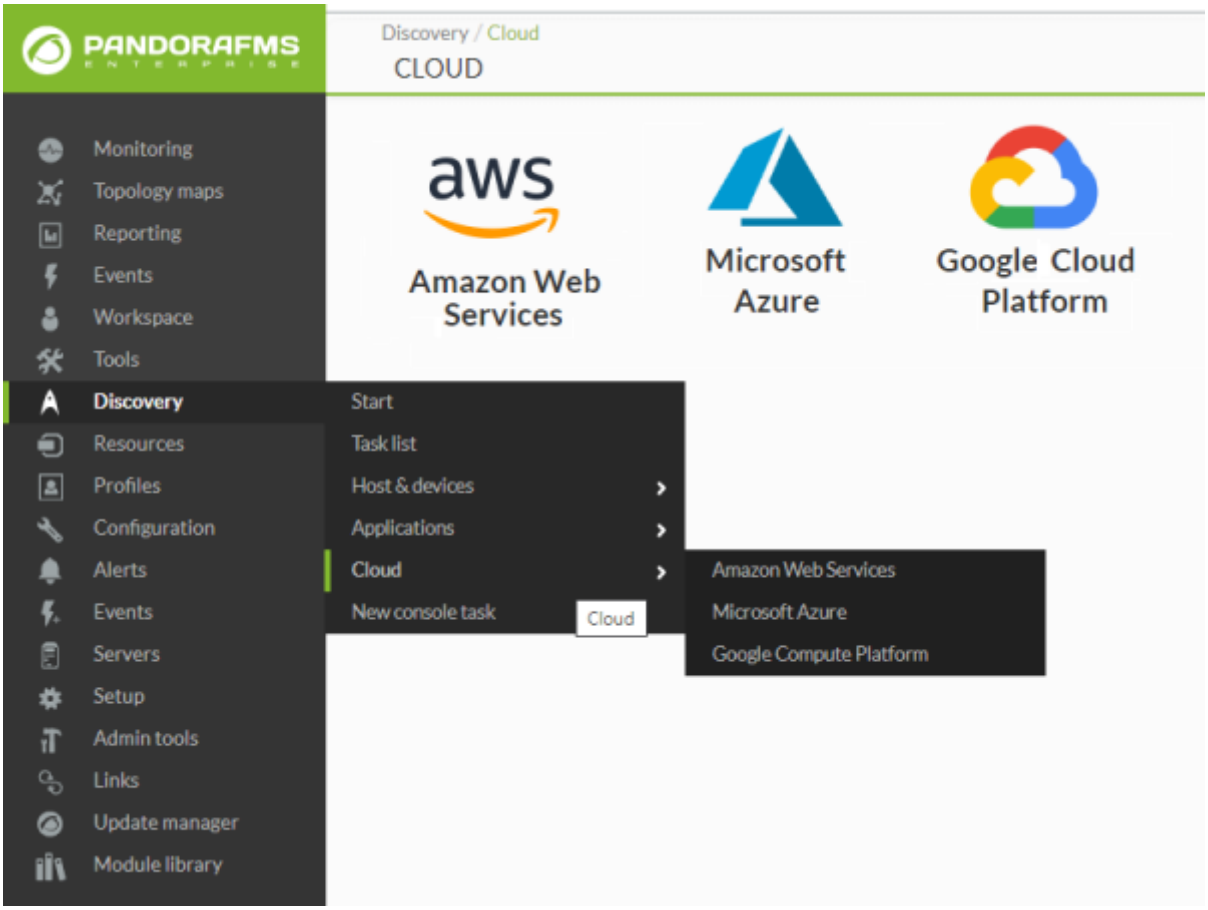
Это позволит получить доступ к разделу Credential store, расположенному в Profiles → Manage agent groups и который будет действовать как хранилище для всех учетных записей Microsoft Azure®, созданных и зарегистрированных ранее.

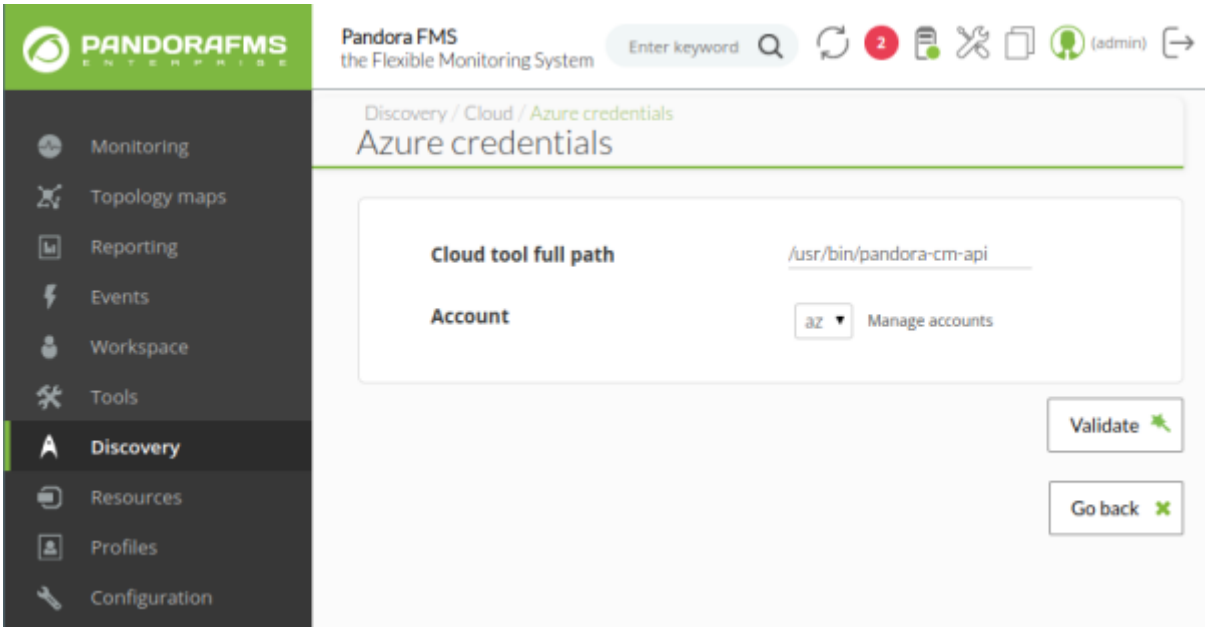
Чтобы установить новую задачу, выполните следующие действия:

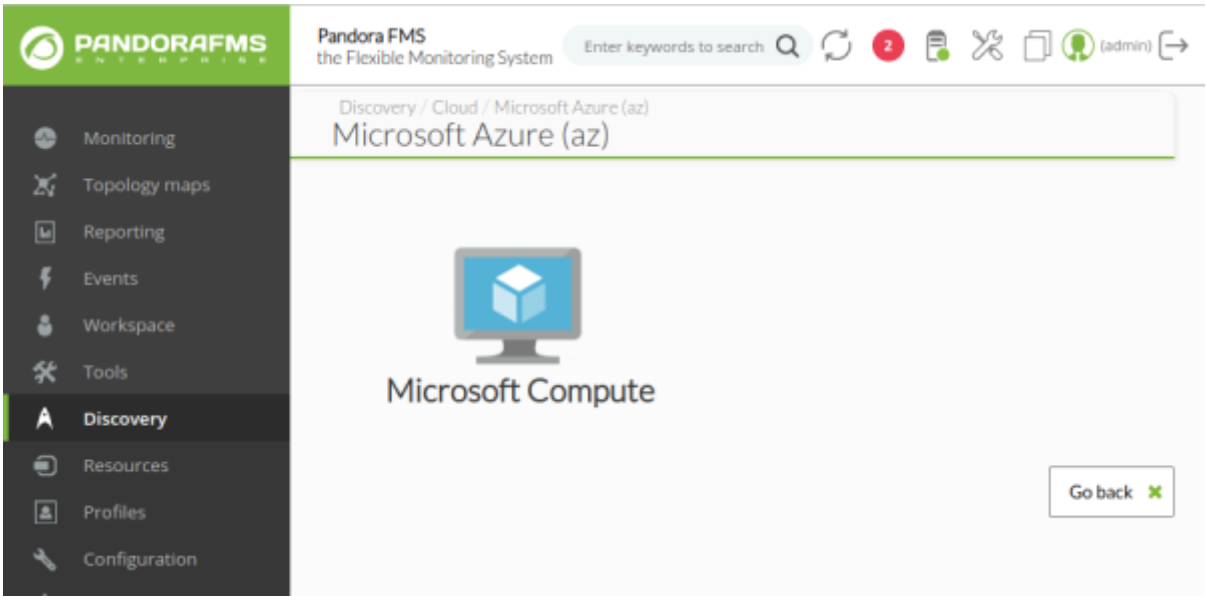
- Добавьте новый ключ в хранилище Credential store.



- Войдите в Discovery > Cloud > Azure и подтвердите учетную запись Azure.

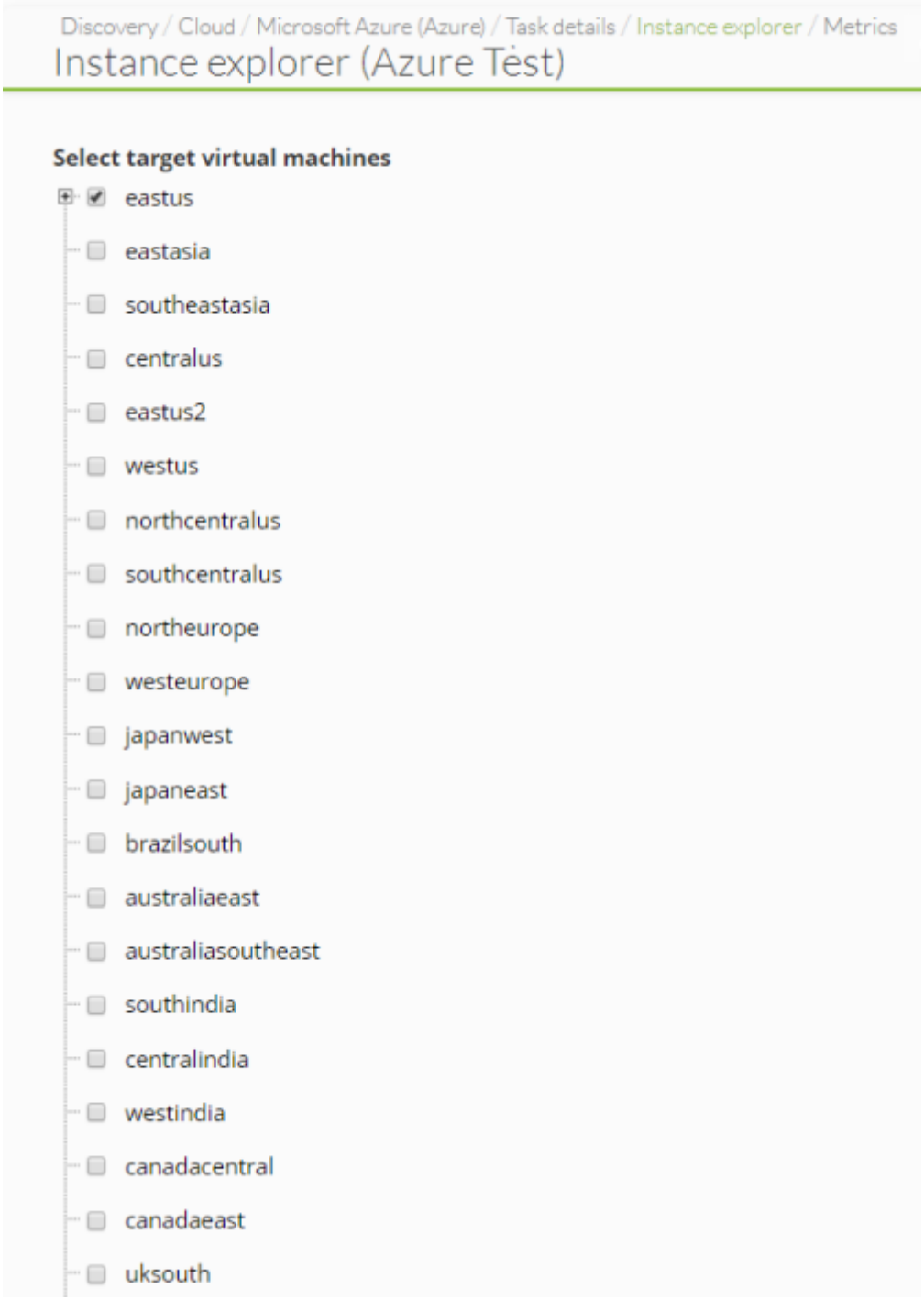

PANDORAFMS
Discovery / Cloud
CLOUD
Monitoring
Topology maps
Reporting
Events
Workspace
Tools
Discovery
Resources
Profiles
Configuration
Alerts
Events
Servers
Setup
Admin tools
Links
Update manager
Module library
aws
Amazon Web Services
Microsoft Azure
Google Cloud Platform
Start
Task list
Host & devices
Applications
Cloud
New console task
Cloud
Amazon Web Services
Microsoft Azure
Google Compute Platform


PANDORAFMS
Pandora FMS
the Flexible Monitoring System
Enter keyword
2
(admin)
Discovery / Cloud / Azure credentials
Azure credentials
Monitoring
Topology maps
Reporting
Events
Workspace
Tools
Discovery
Resources
Profiles
Configuration
Cloud tool full path
/usr/bin/pandora-cm-api
Account
az
Manage accounts
Validate
Go back

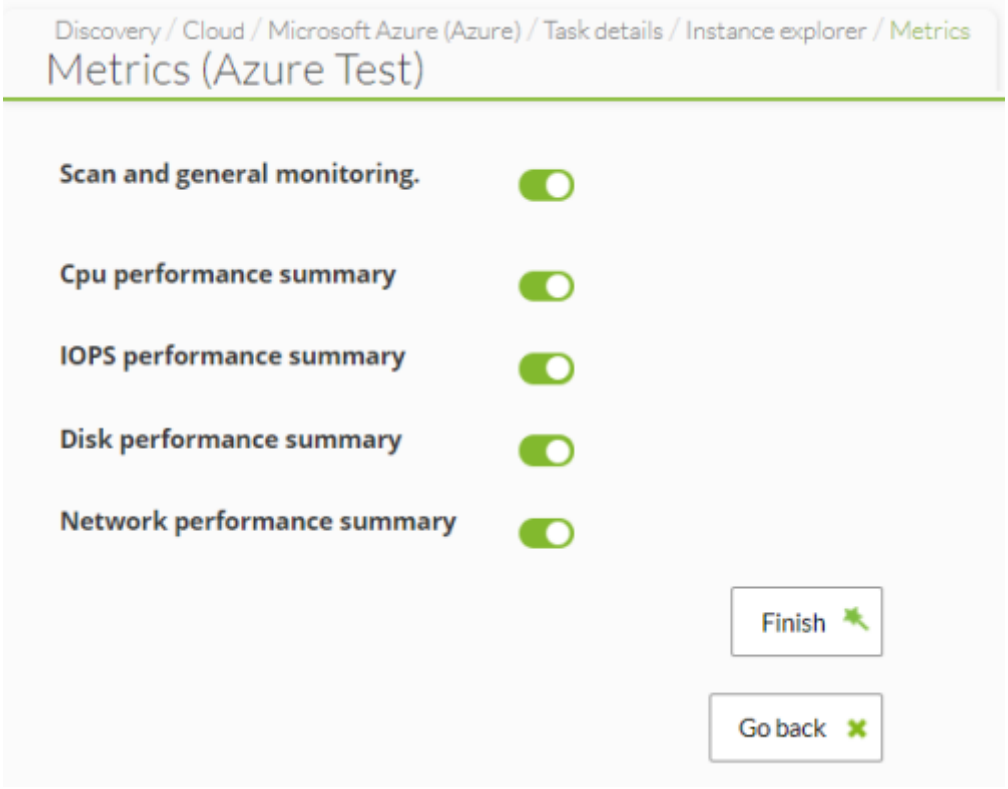


- С этого момента вам нужно определить имя, которое будет иметь задача разведки, сервер, который будет выполнять задачу, группу, к которой она будет принадлежать, и интервал выполнения.

- После определения данных задачи мы выбираем области нашей учетной записи Azure, которые будут отслеживаться. Каждая область позволит нам выбрать нужные экземпляры.



- Последним шагом будет выбор метрик для получения агентов, которые Pandora FMS будет создавать для каждого экземпляра, который она найдет в Microsoft Azure ®. После настройки этого раздела вы можете запустить задачу, и Pandora FMS автоматически создаст агентов в соответствии с экземплярами, запрошенными в предыдущих шагах.



Discovery Cloud: Google Cloud Platform (GCP)

Эта функция доступна начиная с версии 750 Pandora FMS.

Для мониторинга инфраструктуры на Google Cloud Platform® следуйте приведенным ниже пошаговым инструкциям.

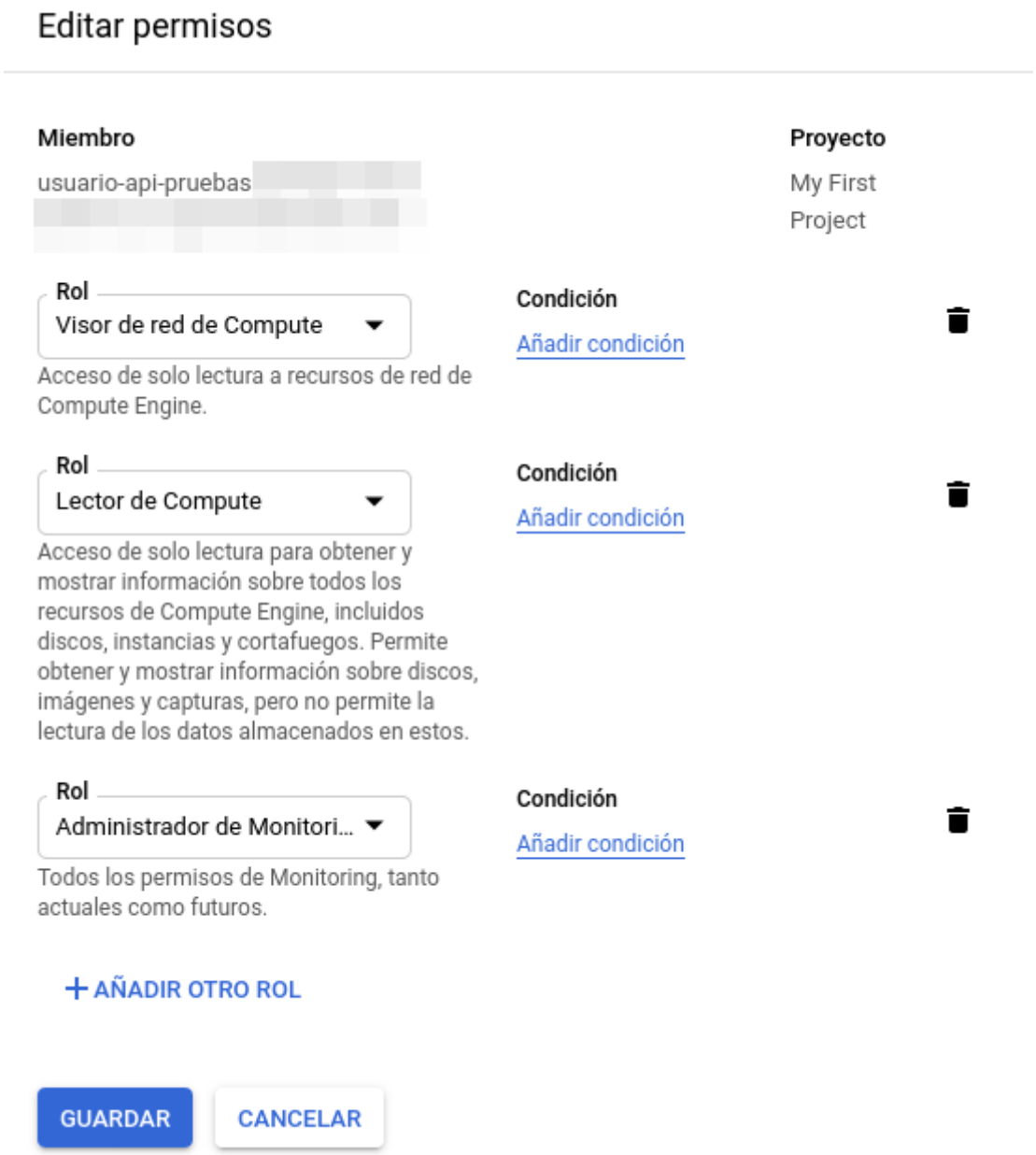
Если у вас версия до 750, перед обновлением необходимо расшифровать базу данных и повторно зашифровать базу данных после обновления.

Если вы перешли с предыдущей версии и уже обновились до Pandora FMS NG 750, вам необходимо частично расшифровать базу данных с помощью `usr/share/pandora_server/utils/pandora_encrypt_db -d -m`, а затем повторно зашифровать ее с помощью `usr/share/pandora_server/utils/pandora_encrypt_db -d`.

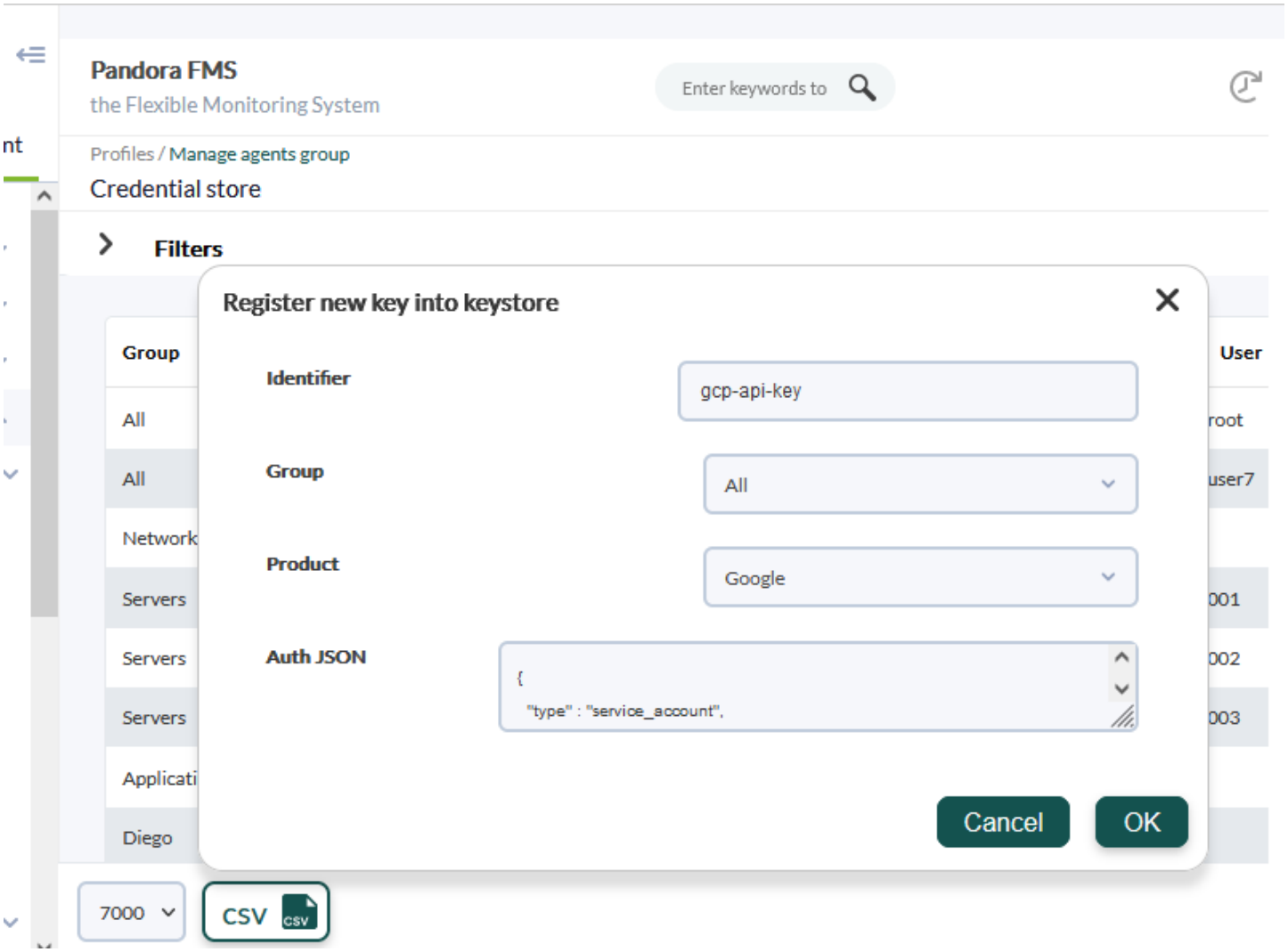
Подтверждение полномочий Google Cloud Platform (GCP)

Для доступа к Google Cloud Console необходимо зарегистрировать JSON-ключ. Выполните следующие действия:

- Зайдите в настройки безопасности в GCP IAM. Учетная запись доступа для регистрации будет служебной учетной записью со следующими привилегиями:

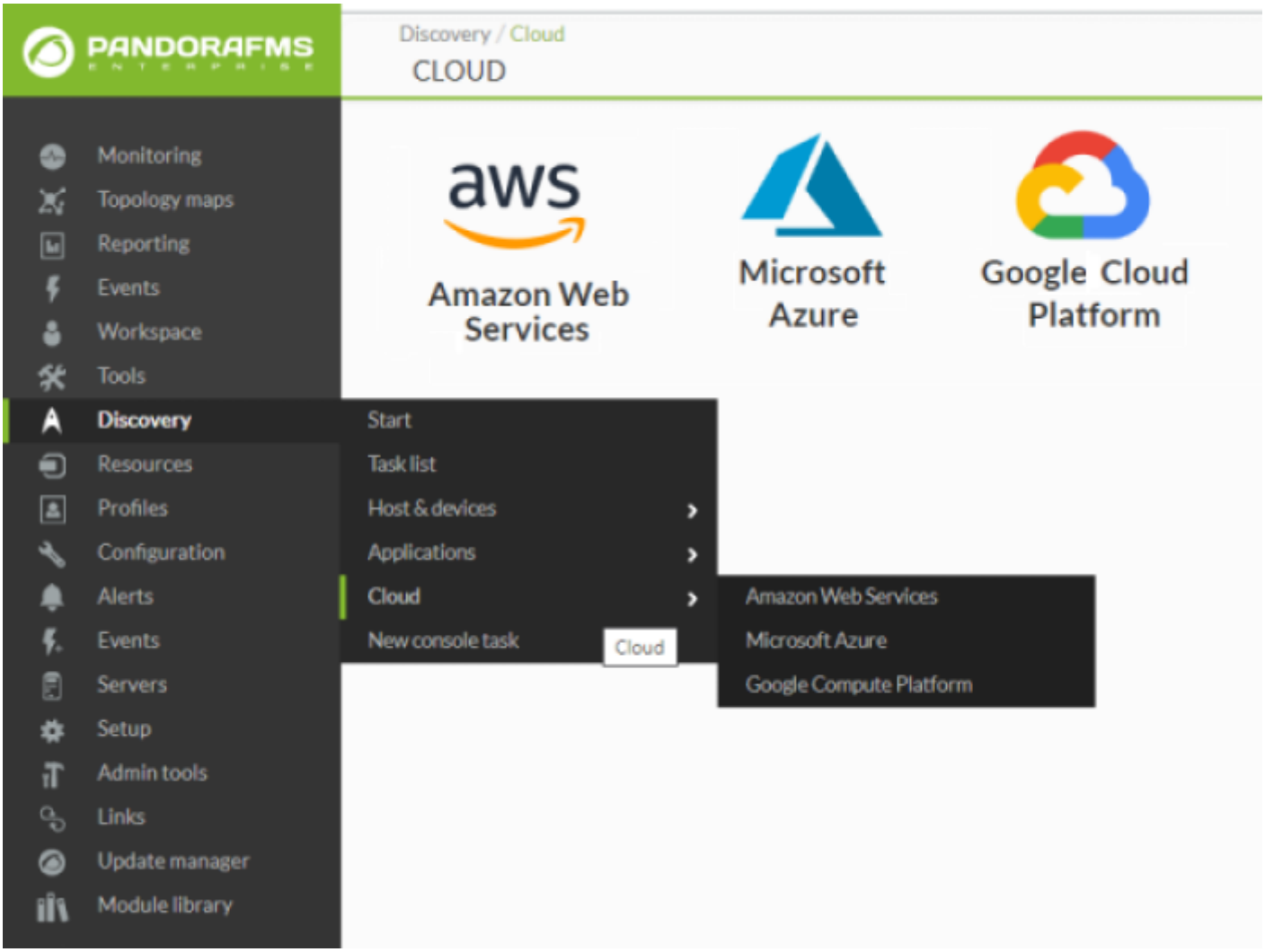


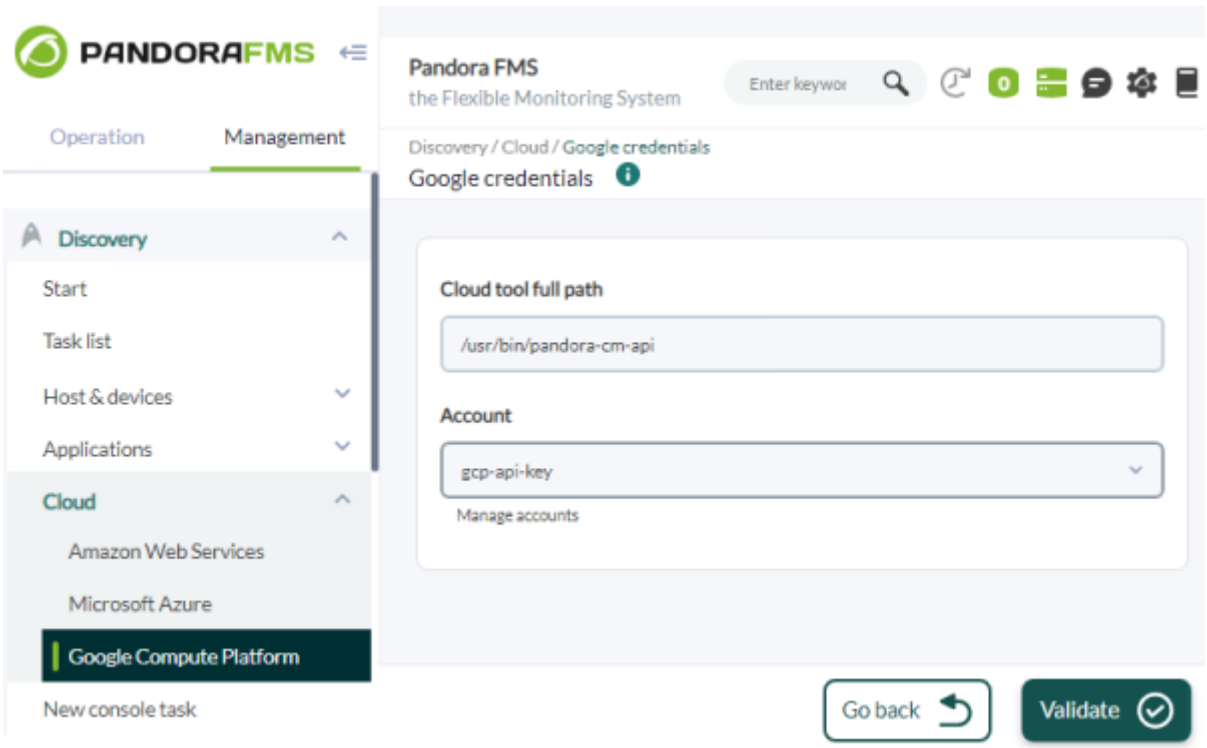
- Зайдите в Pandora FMS в Credential Store, расположенный в Profiles → Manage agent groups → Credential Store и нажмите кнопку «Add key».
- В разворачивающемся Продукте выберите Google и добавьте JSON-ключ учетной записи GCP.

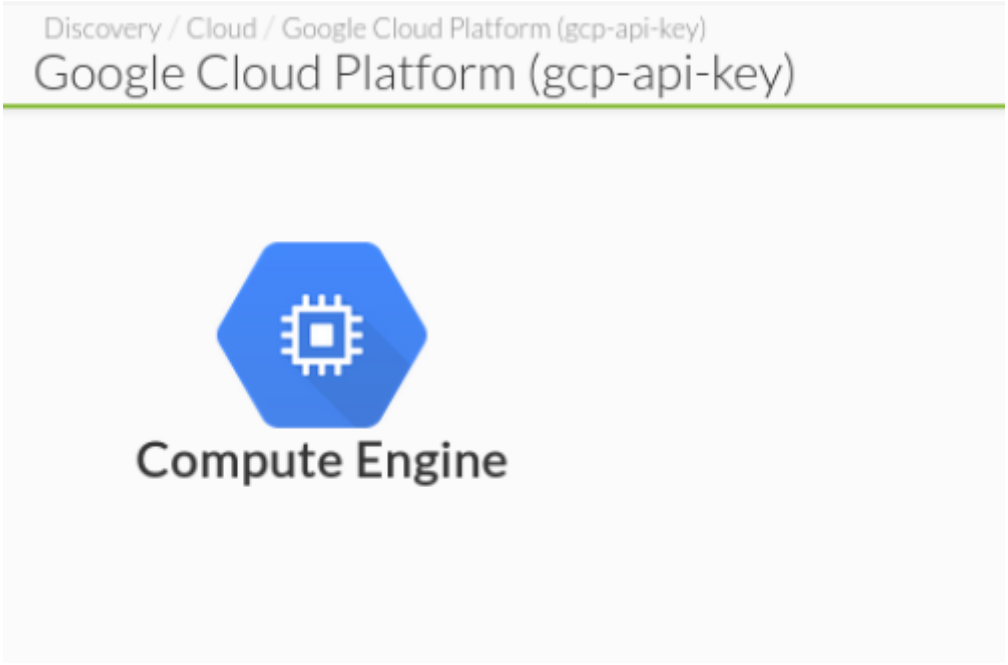


Поле пользователя заполняется автоматически.

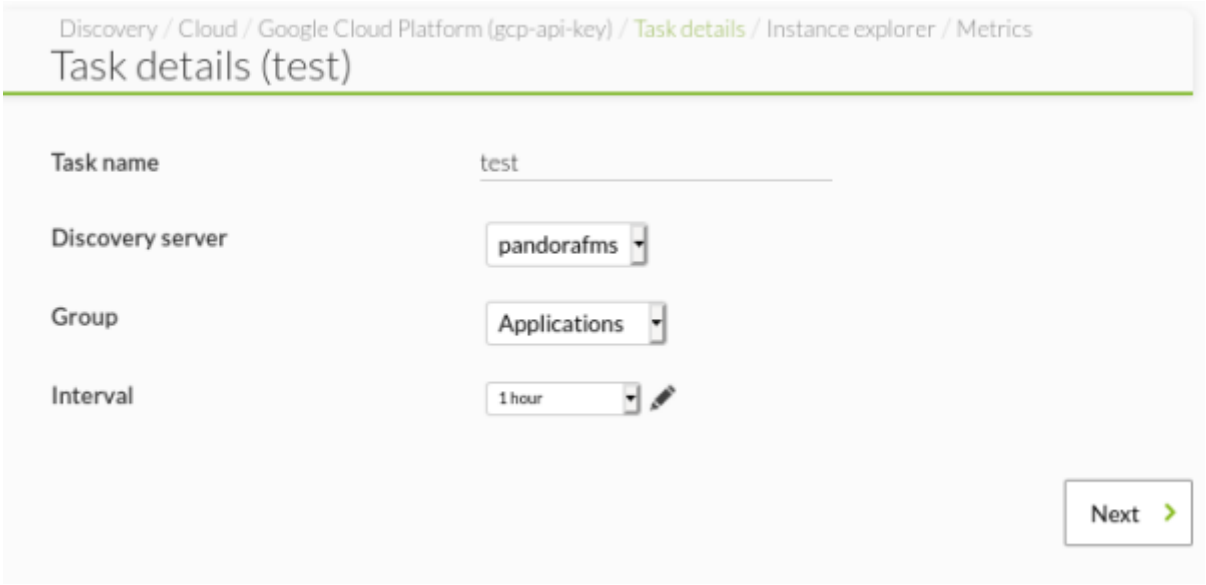
Зайдите в Discovery → Cloud → Google Cloud Platform и подтвердите учетную запись GCP, определив задачу Discovery GCP.


PANDORAFMS
ENTERPRISE
Discovery / Cloud
CLOUD
Monitoring
Topology maps
Reporting
Events
Workspace
Tools
Discovery
Resources
Profiles
Configuration
Alerts
Events
Servers
Setup
Admin tools
Links
Update manager
Module library
aws
Amazon Web Services
Microsoft Azure
Google Cloud Platform
Start
Task list
Host & devices
Applications
Cloud
New console task
Cloud
Amazon Web Services
Microsoft Azure
Google Compute Platform


PANDORAFMS
Pandora FMS
the Flexible Monitoring System
Operation
Management
Discovery / Cloud / Google credentials
Google credentials
Discovery
Start
Task list
Host & devices
Applications
Cloud
Amazon Web Services
Microsoft Azure
Google Compute Platform
New console task
Cloud tool full path
/usr/bin/pandora-cm-api
Account
gcp-api-key
Manage accounts
Go back
Validate

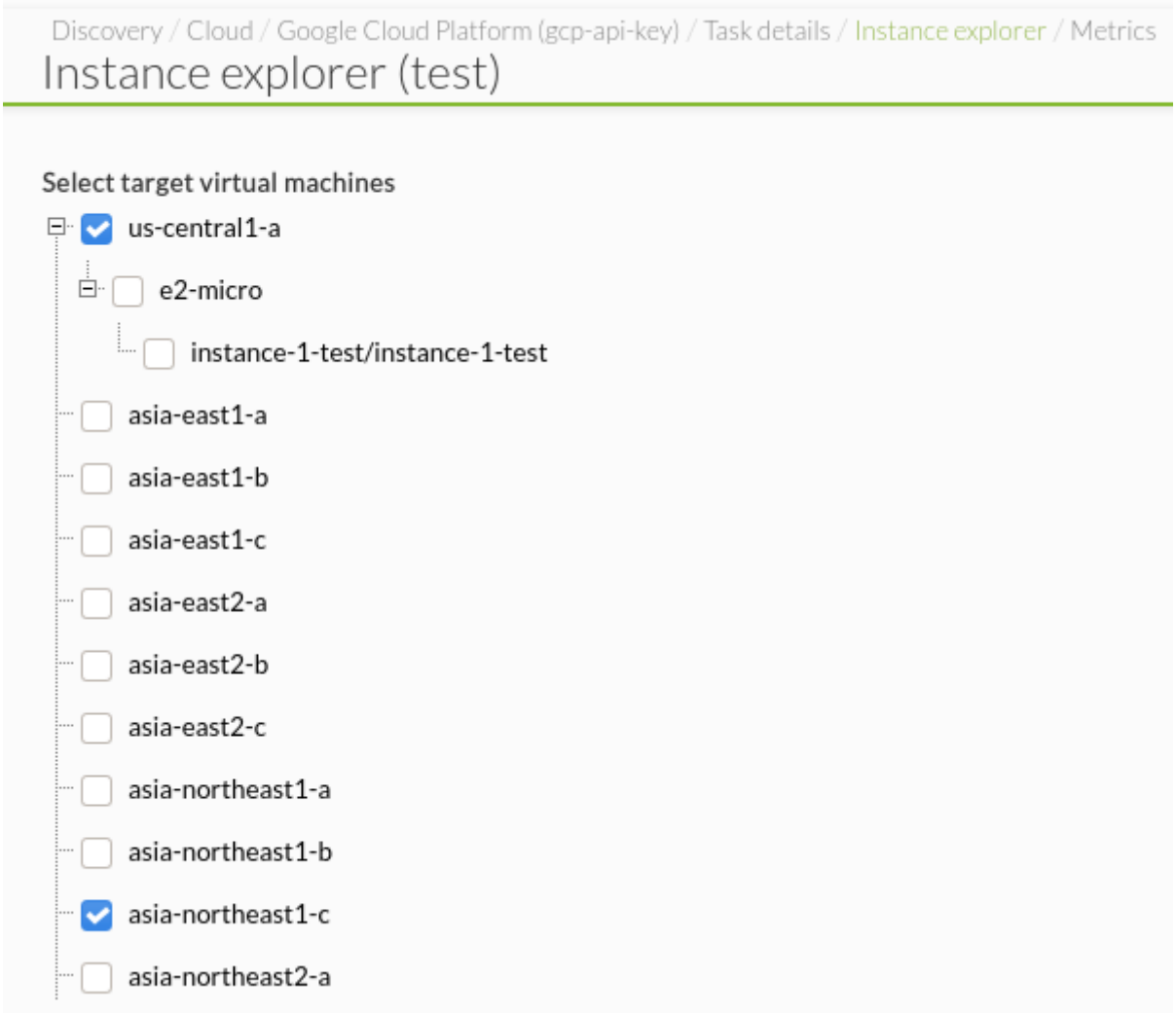


Настроить задачу в Pandora FMS



- Task name: Определите имя для задачи.
- Discovery server: Выберите сервер, который будет выполнять мониторинг.
- Group: Назначьте группу.
- Interval: Укажите частоту выполнения задачи.

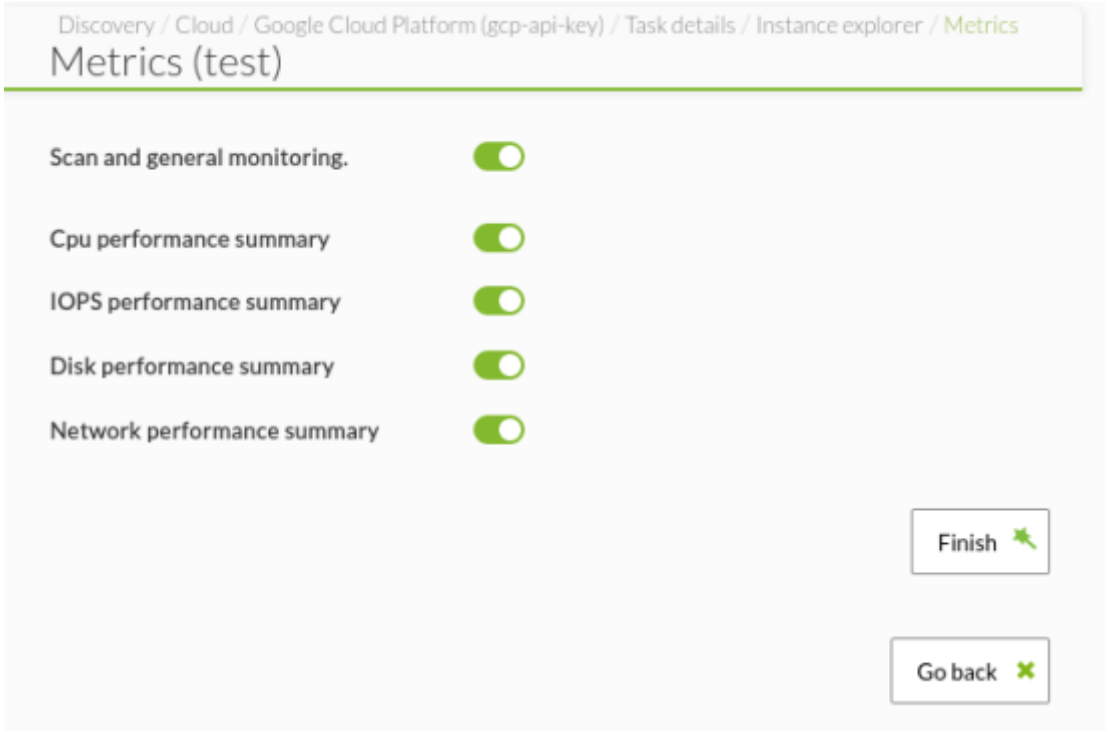
После определения данных задачи выберите области нашего аккаунта GCP, которые будут контролироваться. Каждая область позволит нам выбрать нужные экземпляры.



При выборе зоны автоматически будут отслеживаться новые экземпляры, обнаруженные в этой зоне.

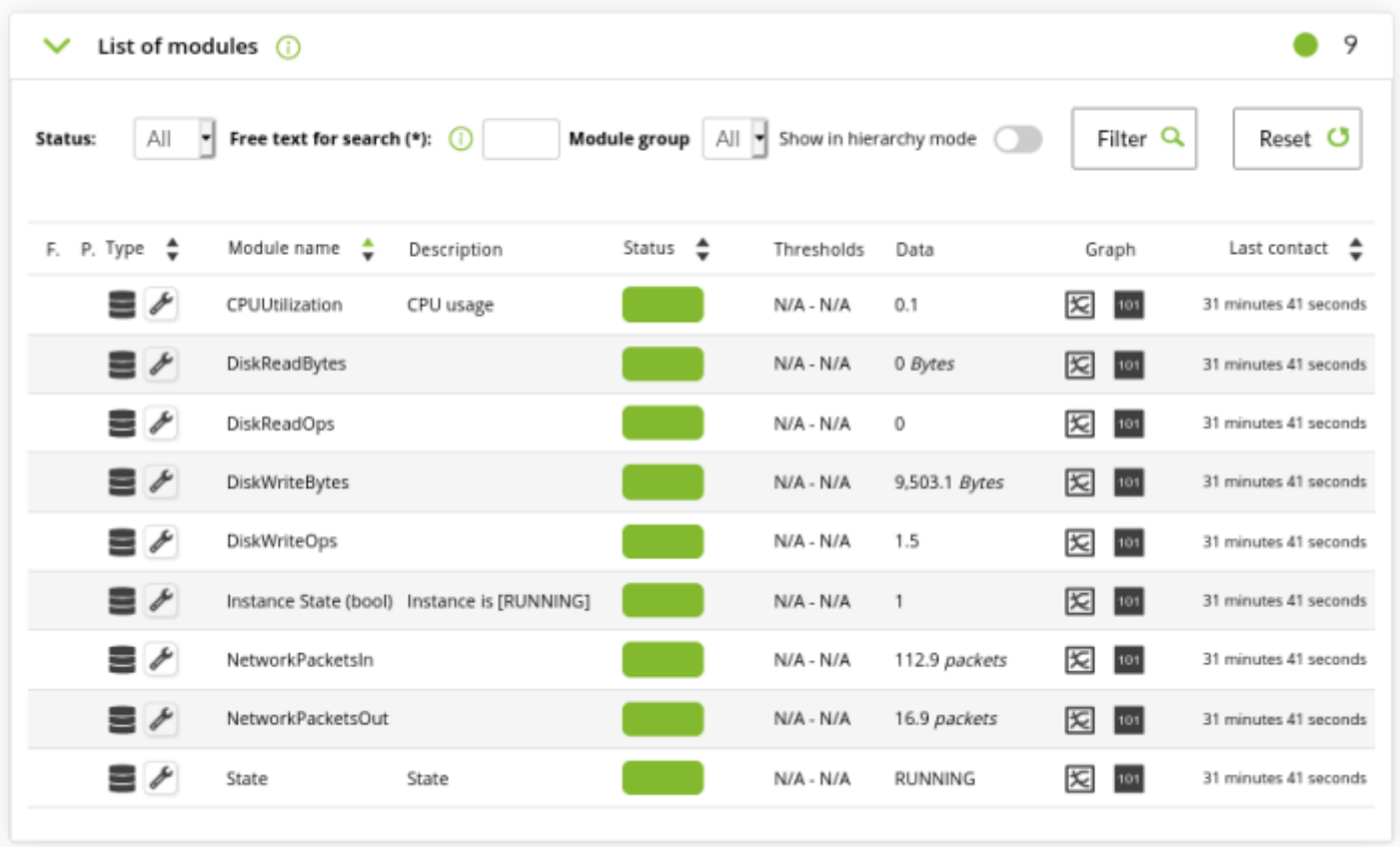
При выборе экземпляра он будет повергаться заметному мониторингу, даже если его зона не контролируется.

Последний шаг заключается в выборе метрик для получения агентов, которые Pandora FMS будет создавать для каждого экземпляра, который она найдет в Google Cloud Platform®. После настройки этого раздела вы можете запустить задачу, и Pandora FMS автоматически создаст агентов в соответствии с экземплярами, запрошенными в предыдущих шагах.



Как и в Azure или AWS, будет *шаблонный* агент под названием Google или GCP, в котором появятся все модули, связанные с мониторингом Google.

Ниже приведены некоторые метрики, которые он собирает с экземпляров:

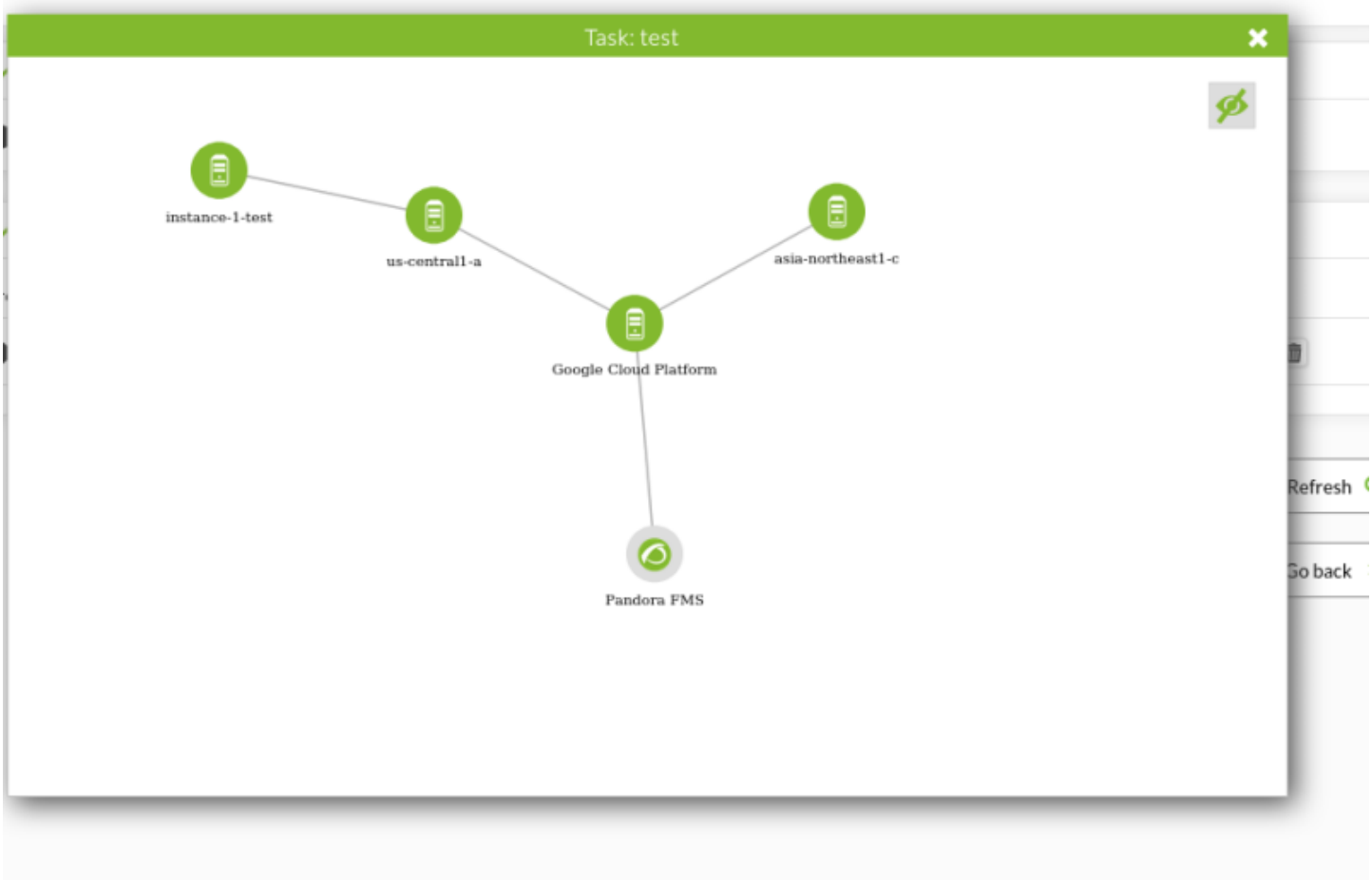


F.	P.	Type	Module name	Description	Status	Thresholds	Data	Graph	Last contact
			CPUUtilization	CPU usage		N/A - N/A	0.1		31 minutes 41 seconds
			DiskReadBytes			N/A - N/A	0 *Bytes*		31 minutes 41 seconds
			DiskReadOps			N/A - N/A	0		31 minutes 41 seconds
			DiskWriteBytes			N/A - N/A	9,503.1 *Bytes*		31 minutes 41 seconds
			DiskWriteOps			N/A - N/A	1.5		31 minutes 41 seconds
			Instance State (bool)	Instance is [RUNNING]		N/A - N/A	1		31 minutes 41 seconds
			NetworkPacketsIn			N/A - N/A	112.9 *packets*		31 minutes 41 seconds
			NetworkPacketsOut			N/A - N/A	16.9 *packets*		31 minutes 41 seconds
			State	State		N/A - N/A	RUNNING		31 minutes 41 seconds

Те экземпляры, которые исчезнут из области, которая постоянно контролируется мониторингом, появятся в критическом состоянии или *removed*, а все остальные

модули - в неизвестном. В случае если весь экземпляр переходит в состояние неизвестности, вы можете использовать режим auto-disable..

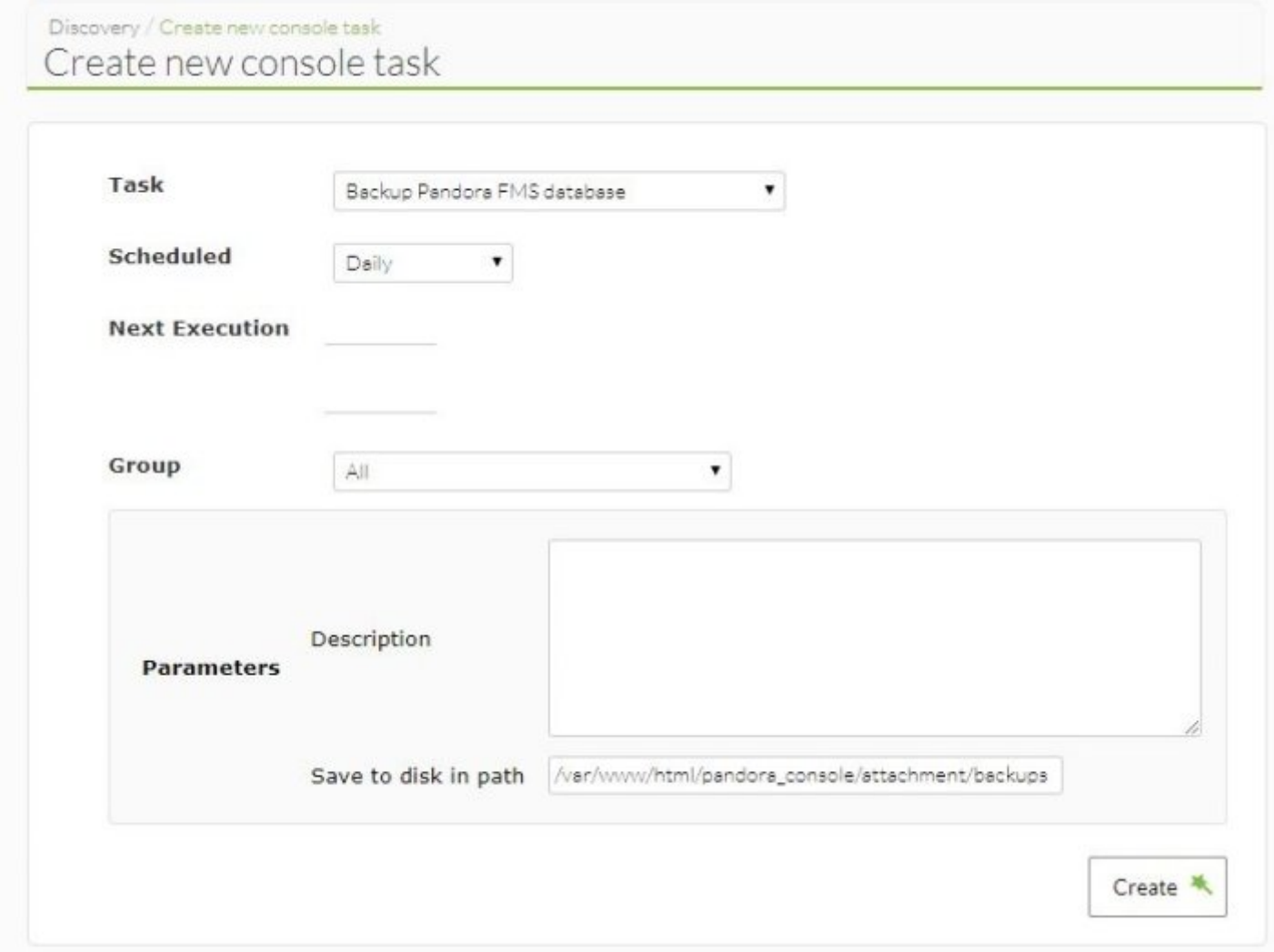
Вы также можете просмотреть карту из списка задач GCP.



Discovery Console Tasks

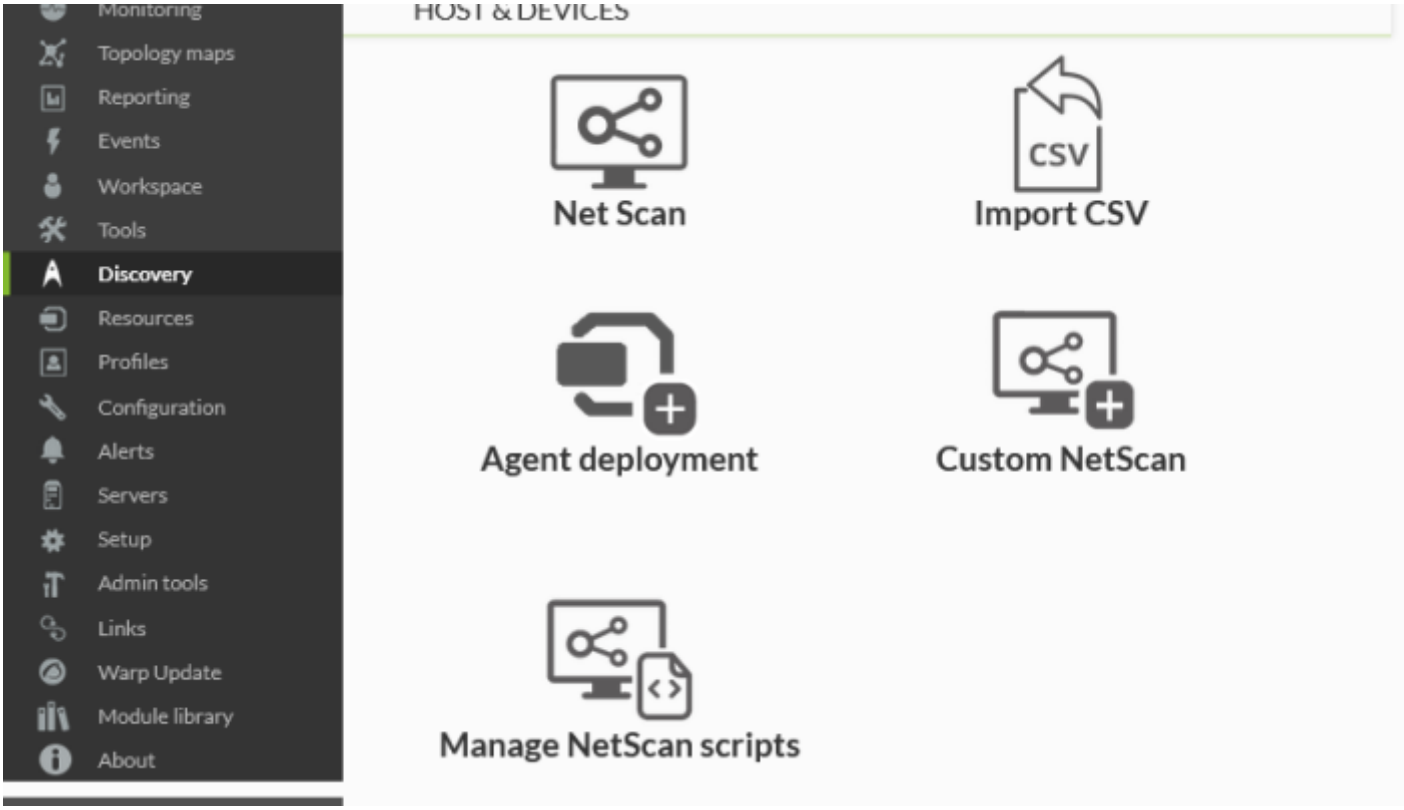
Вернуться наверх ♦

По аналогии с Task List, Console Tasks позволяет создавать новые задания с учетом следующих параметров:



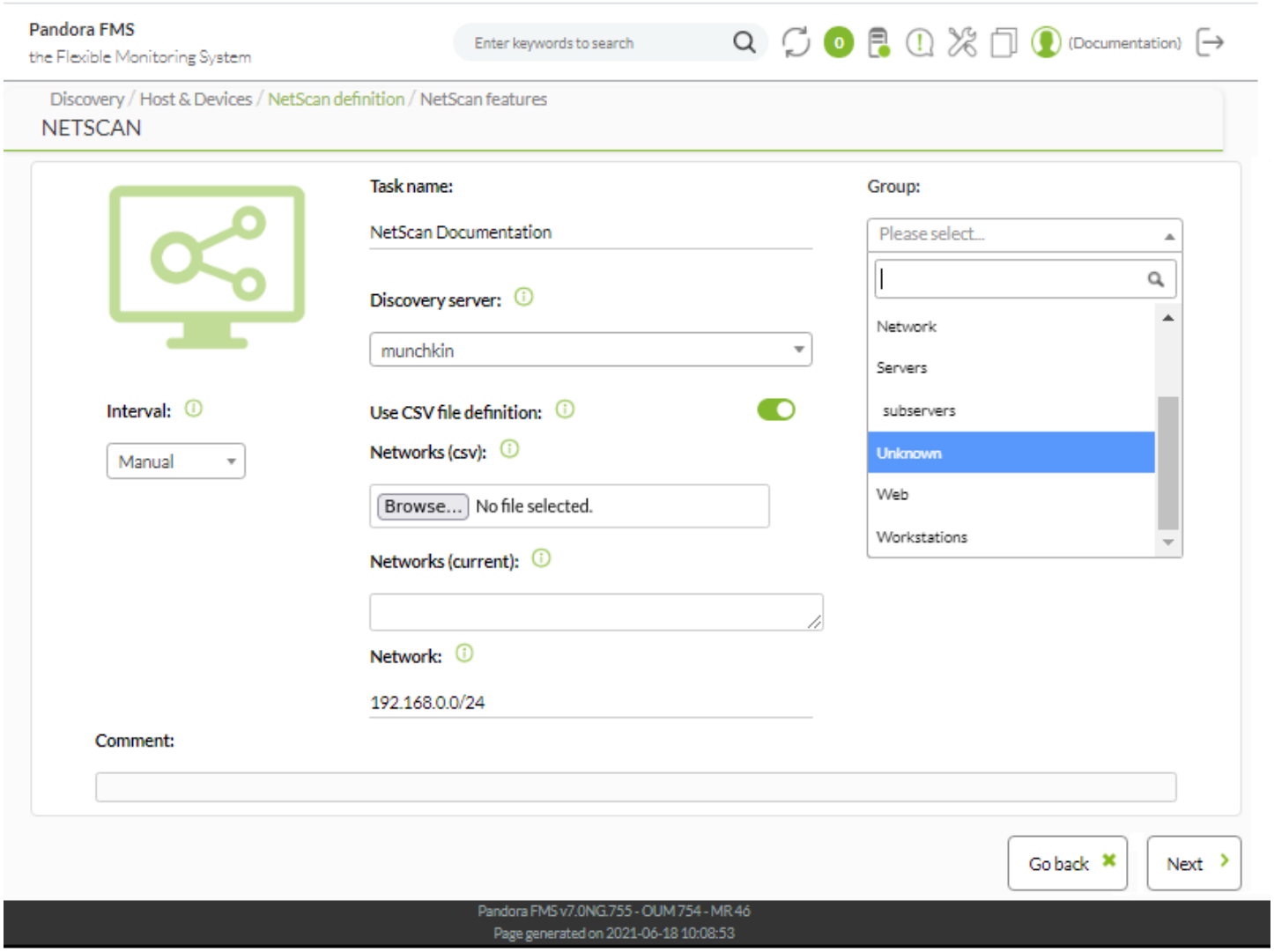
Discovery Host&Devices

Вернуться наверх ♦



NetScan

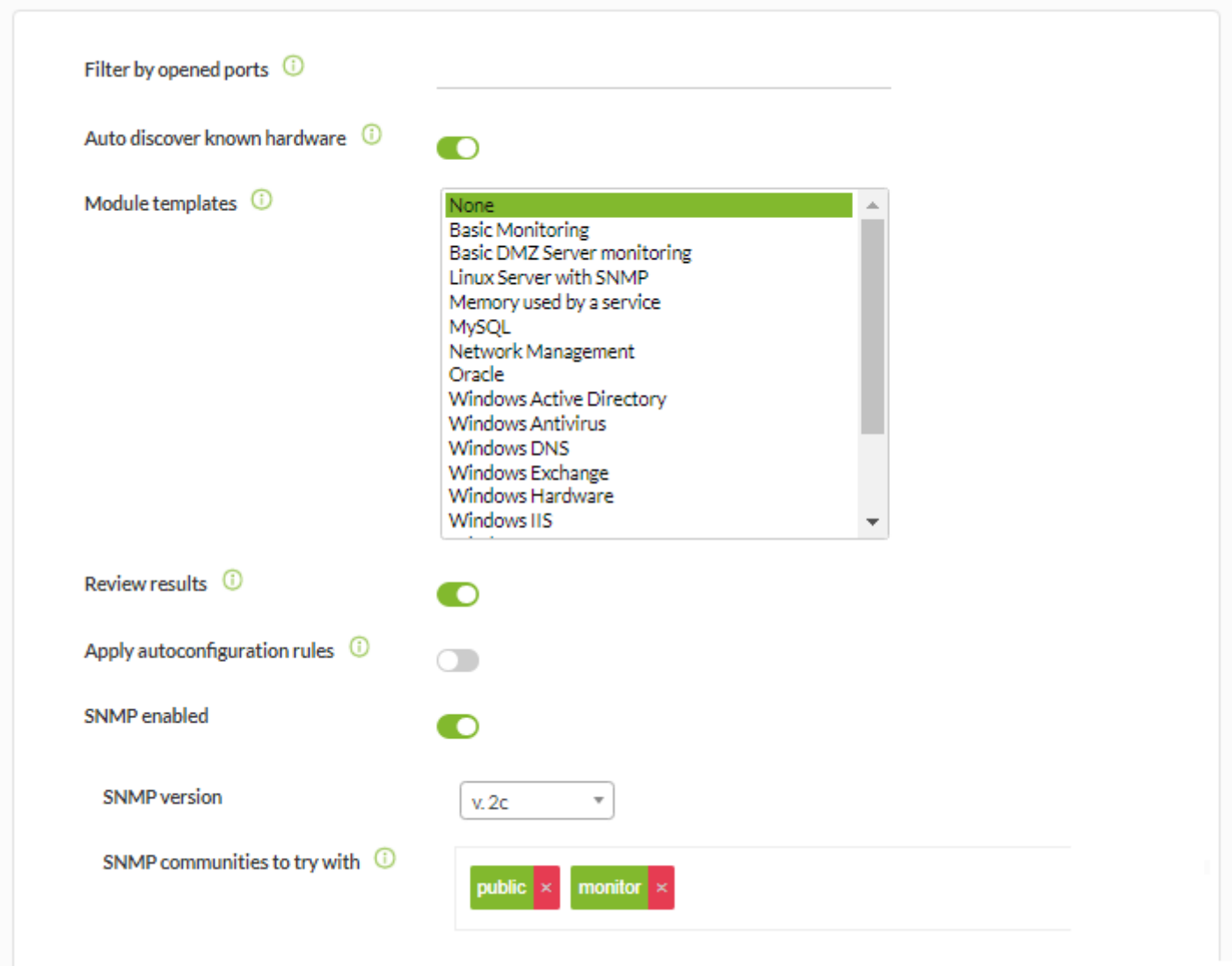
NetScan позволяет обнаруживать устройства в сети и применять к ним различные правила мониторинга. Вы можете узнать больше из обучающего видеоролика «Обнаружение устройств и загрузка агентов с помощью Pandora FMS: Discovery Host&Devices».



При создании задания группа, к которой оно будет принадлежать, задается заранее, а при распознавании необходимо выбрать между загрузкой файла в формате CSV с конкретными устройствами для проверки (Use CSV file definition:) или сетью (Network:).

Интервалы, выбранные как ручные, должны запускаться вручную. Discovery не запустит ручное задание автоматически.

раздел характеристики имеет несколько вариантов на одном экране (следующий пример разделен в дидактических целях):



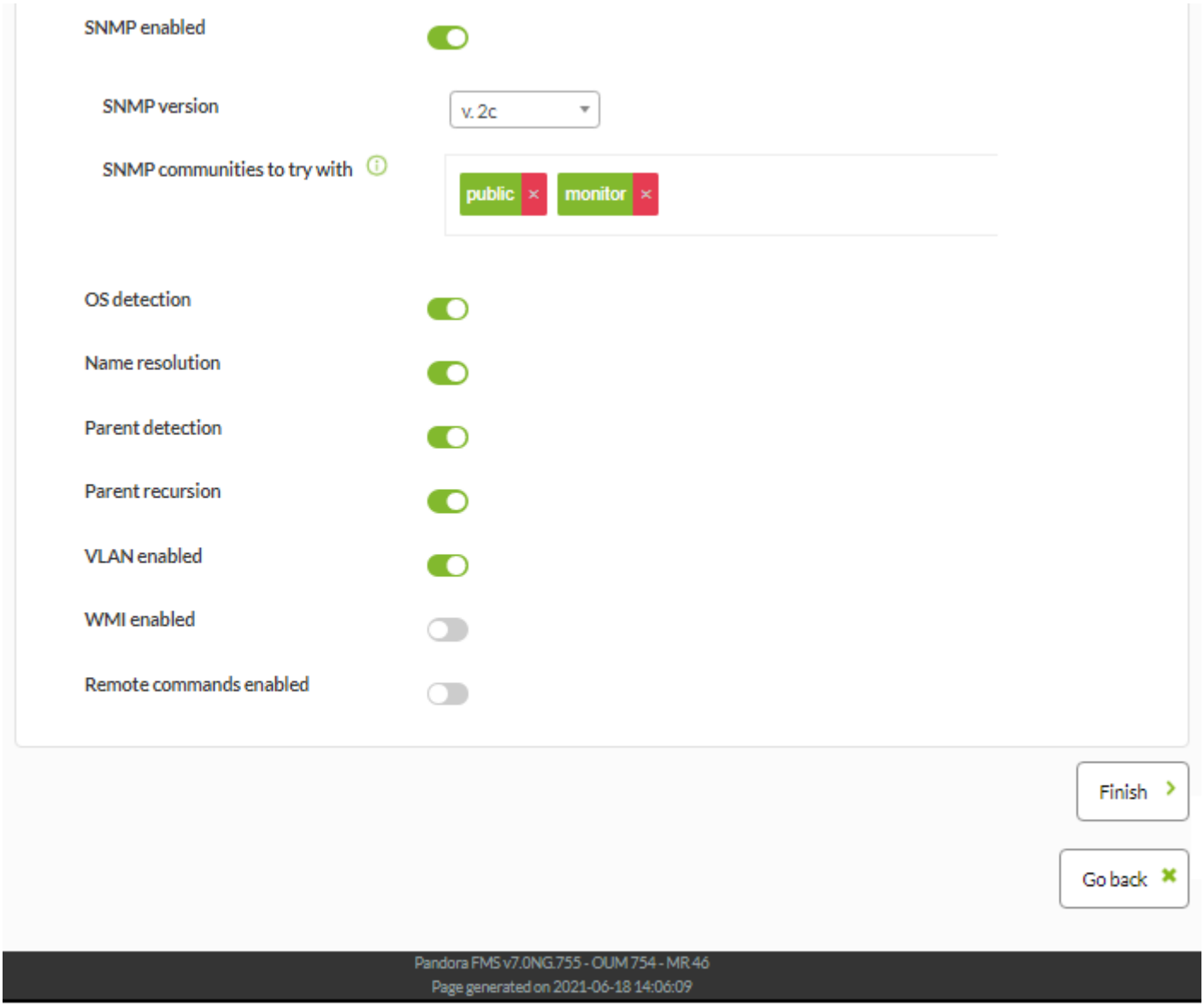
- Auto discover known hardware: Автообнаружение известного оборудования динамически применяет добавленные шаблоны, которые были добавлены посредством Private Enterprise Number.
- Modules templates: Пробует применить модули выбранных шаблонов. Если выполнение не пройдет тест, оно не будет добавлено в список мониторинга.
- Review results: Пользователь должен подтвердить результаты, выбрав, какие агенты будут созданы из тех, которые были найдены задачей обнаружения.
- Apply autoconfiguration rules: Применяет ранее определенные правила автоматической настройки к обнаруженным агентам.

Автоматическая настройка позволяет применять политики, изменения групп и конфигурации, а также запускать пользовательские события или выполнять *скрипты* в действиях.

Агенты, обнаруженные NetScan, являются удаленными агентами без конфигурационного файла. Вы не сможете применить локальные политики мониторинга или добавить массовые изменения конфигурации, если

вы не развернете агента в целях.

- SNMP enabled: Чтобы дополнить информацию, полученную от обнаруженных сетевых устройств, необходимо включить SNMP. Это улучшает обнаружение путем изучения информации SNMP, доступной в обнаруженных целях. При включении этого *токена* появятся две дополнительные опции:
  - Версия SNMP: Необходимо выбрать версию SNMP (1,2, 2c и 3), настроенную на устройствах сканируемой сети.
  - SNMP communities to try with: Необходимо указать сообщество, сконфигурированное в среде. Вы можете добавить столько сообществ, сколько вам нужно, в соседнее поле.



- WMI enabled: Сканирование WMI может быть включено. Учетные данные должны быть выбраны в Credentials to try with, которые ранее были загружены в хранилище ключей.

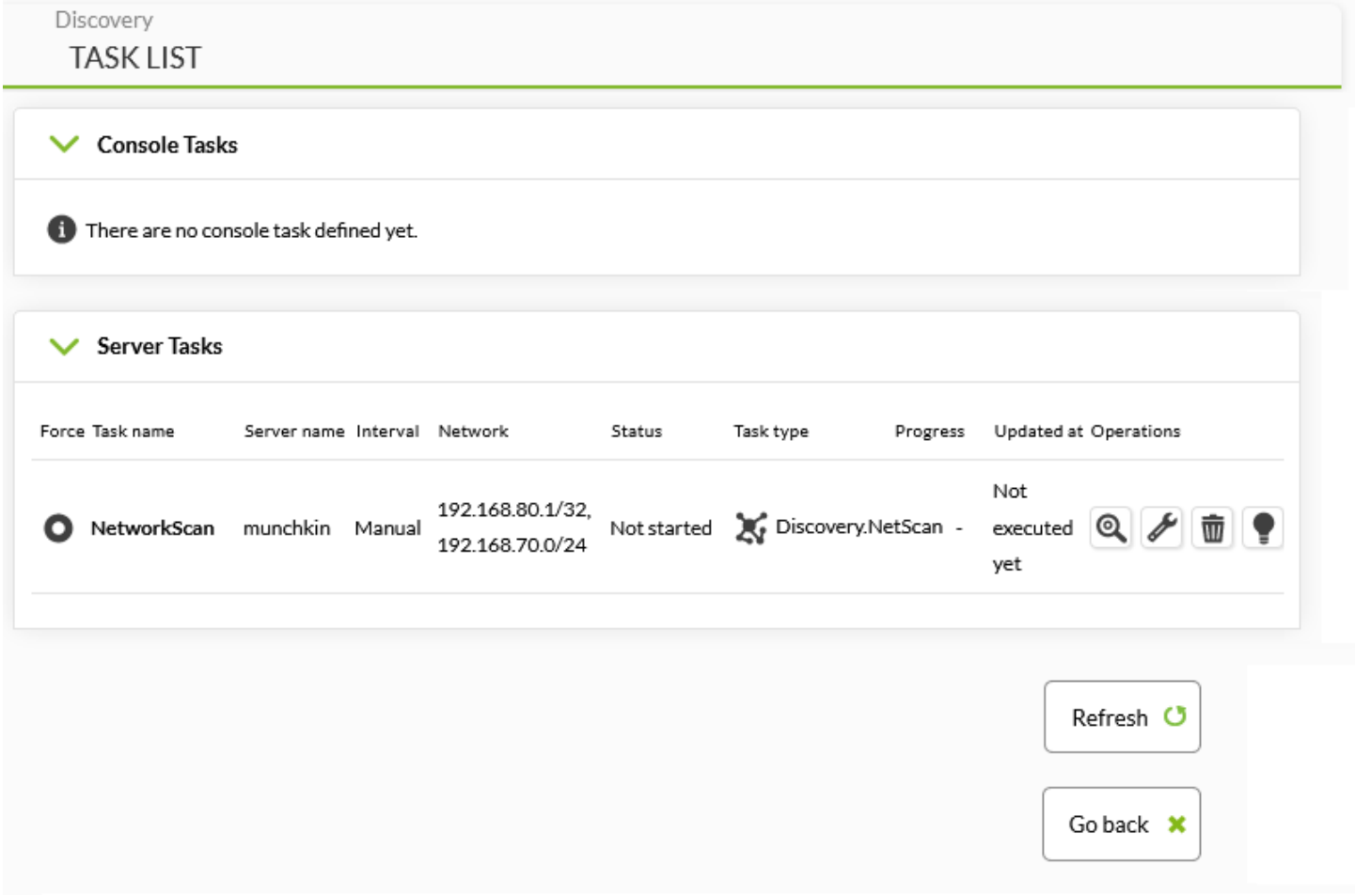
Различные предоставленные учетные данные будут проверены на обнаруженных объектах, поддерживающих WMI, дополняя мониторинг

модулями, которые сообщают об использовании процессора, памяти и диска.

* OS detection: Определите целевую операционную систему.

- Name resolution: Определить имя цели.
- Parent detection: С помощью информации, собранной SNMP, рассчитываются различные взаимосвязи между устройствами, чтобы представить вашу сетевую инфраструктуру.
- Parent recursion: Улучшает обнаружение родителей путем добавления рекурсии в процесс.
- VLAN enabled: Определяет сети VLAN, к которым подключены различные устройства.

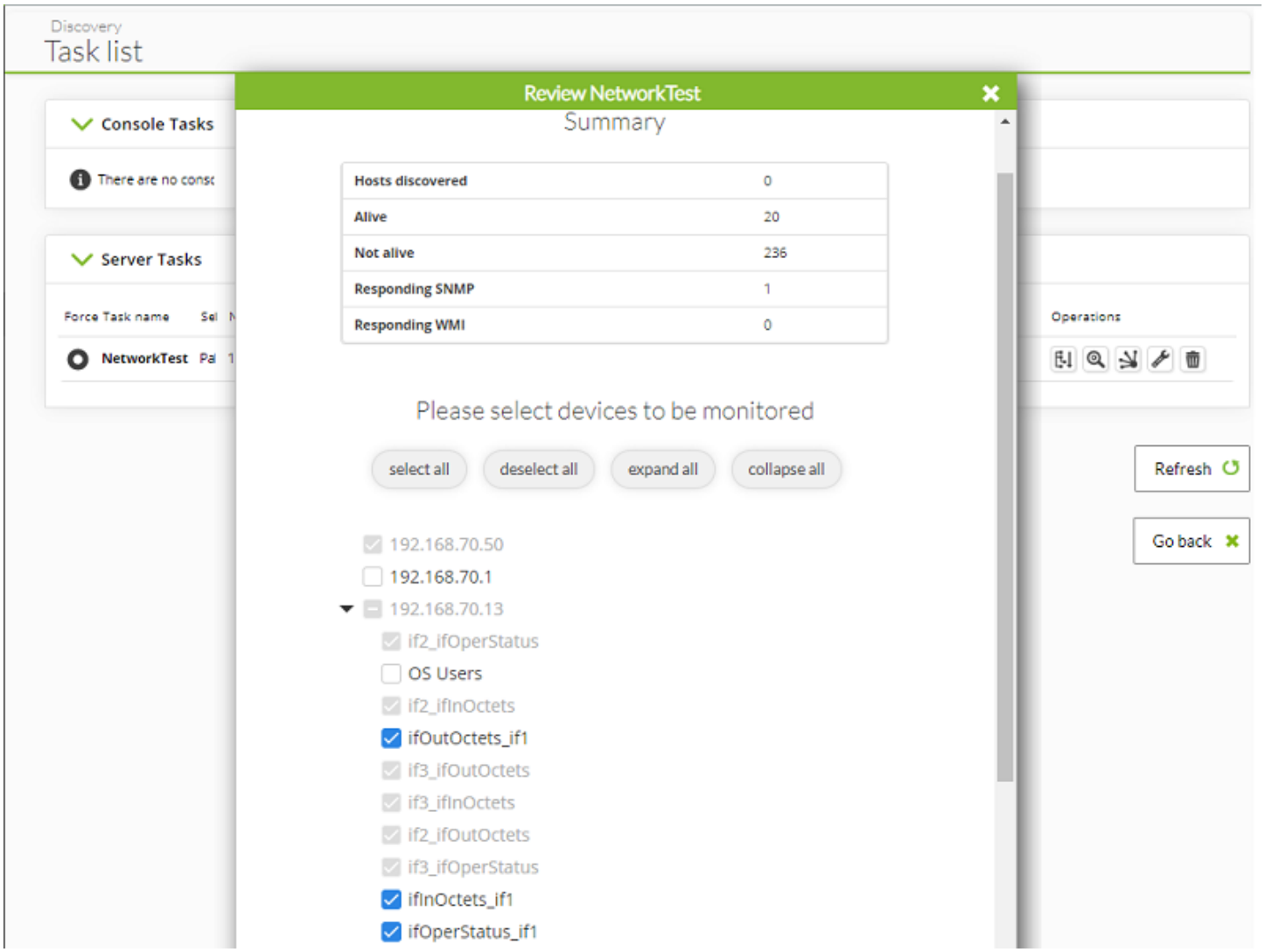
После завершения работы помощника, Discovery начнет запускаться через каждый заданный интервал времени. Если интервал задан вручную, задание должно быть запущено вручную:



После завершения задачи, если вы зашли в раздел Review, вы увидите сводку найденных устройств, реагирующих на ping или fping и другие метрики, доступные через SNMP или WMI. Будут показаны все IP, каждый из которых находится в одном из этих двух состояний:

- Отключен: В среде мониторинга уже есть агент или модуль, и он не создан или не изменен.
- Включено: Новый элемент, который не подвергается мониторингу, или в полученных метриках появился новый модуль, который вы увидите в выпадающем списке. В устройствах, которые находятся в этом состоянии, вы можете выбрать, добавить ли его в список контролируемых

агентов или ,если вы хотите, добавить любую из новых включенных метрик.

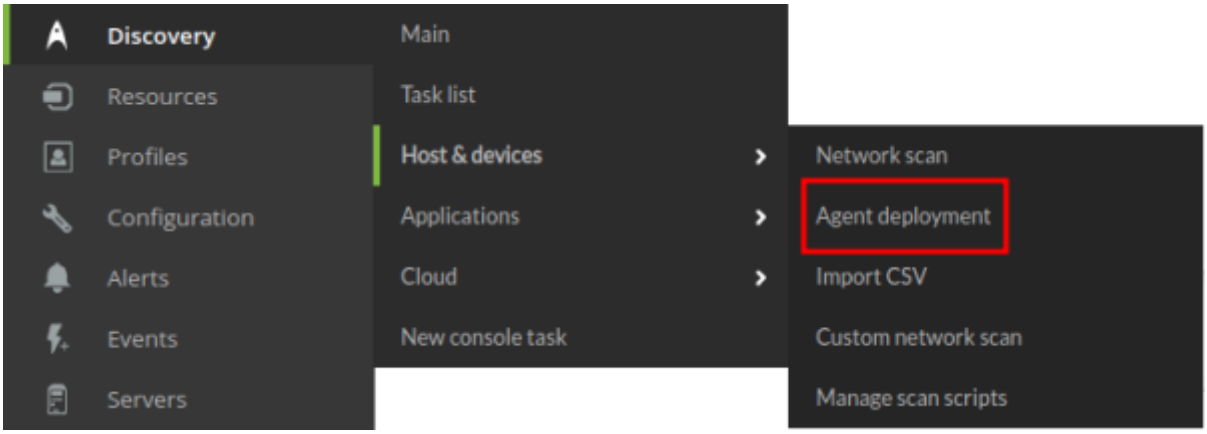


После выбора целей, подлежащих мониторингу, система систематически создает их. Во время этого процесса определяется операционная система цели, чтобы дополнить уже собранную информацию.

Автоматическое развертывание агентов

Версия NG 737 или выше.

Вы можете узнать больше из обучающего видеоролика «Обнаружение устройств и загрузка агентов с помощью Pandora FMS: Discovery Host&Devices».



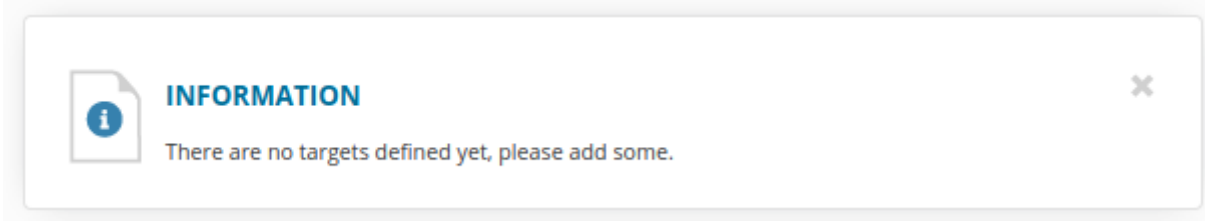
Для работы автоматического развертывания агентов необходимо, чтобы сервер был версии EL7 (Red Hat Enterprise Linux) или выше.

В GNU/Linux Debian и родственных дистрибутивах (Ubuntu и т.д.) *у вас уже должна быть установлена команда* curl.

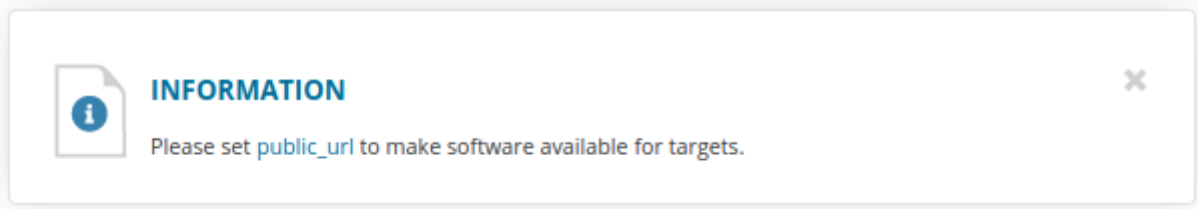
Ниже описаны шаги по развертыванию программных агентов из консоли:

- Зарегистрируйте версии программных агентов для развертывания в репозитории агентов : Вам понадобятся инсталляторы агентов для развертывания. Вы также можете использовать пользовательские агенты.
- Зарегистрируйте учетные данные, которые будут использоваться для подключения к целям в в менеджере учетных данных: Вам необходимо указать учетные данные, с помощью которых будет проверяться доступ к найденным или указанным целям.
- Подтвердите готовность среды к развертыванию:
  - Вы должны определить цели для развертывания.
  - Вы должны определить адрес публичного доступа.
  - Вы должны зарегистрировать инсталляторы для развертывания программного обеспечения.

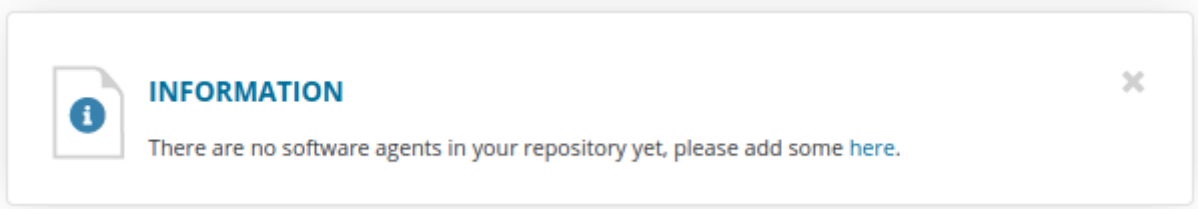
Из-за этих трех последних пунктов при первом посещении центра развертывания вы увидите следующие предупреждения:



Эти цели будут определены в соответствии с инструкциями в следующих разделах



В предыдущем сообщении предлагается ссылка (public_url), которая ведет к настройке публичного URL сервера Pandora FMS.



В сообщении выше приведена ссылка (here), которая ведет к настройке инсталляторов Программных Агентов для каждой отдельной среды.

Эта система не выполняет операции PUSH; все развертывания передаются через *предложение* программного обеспечения и указанием цели установить его.

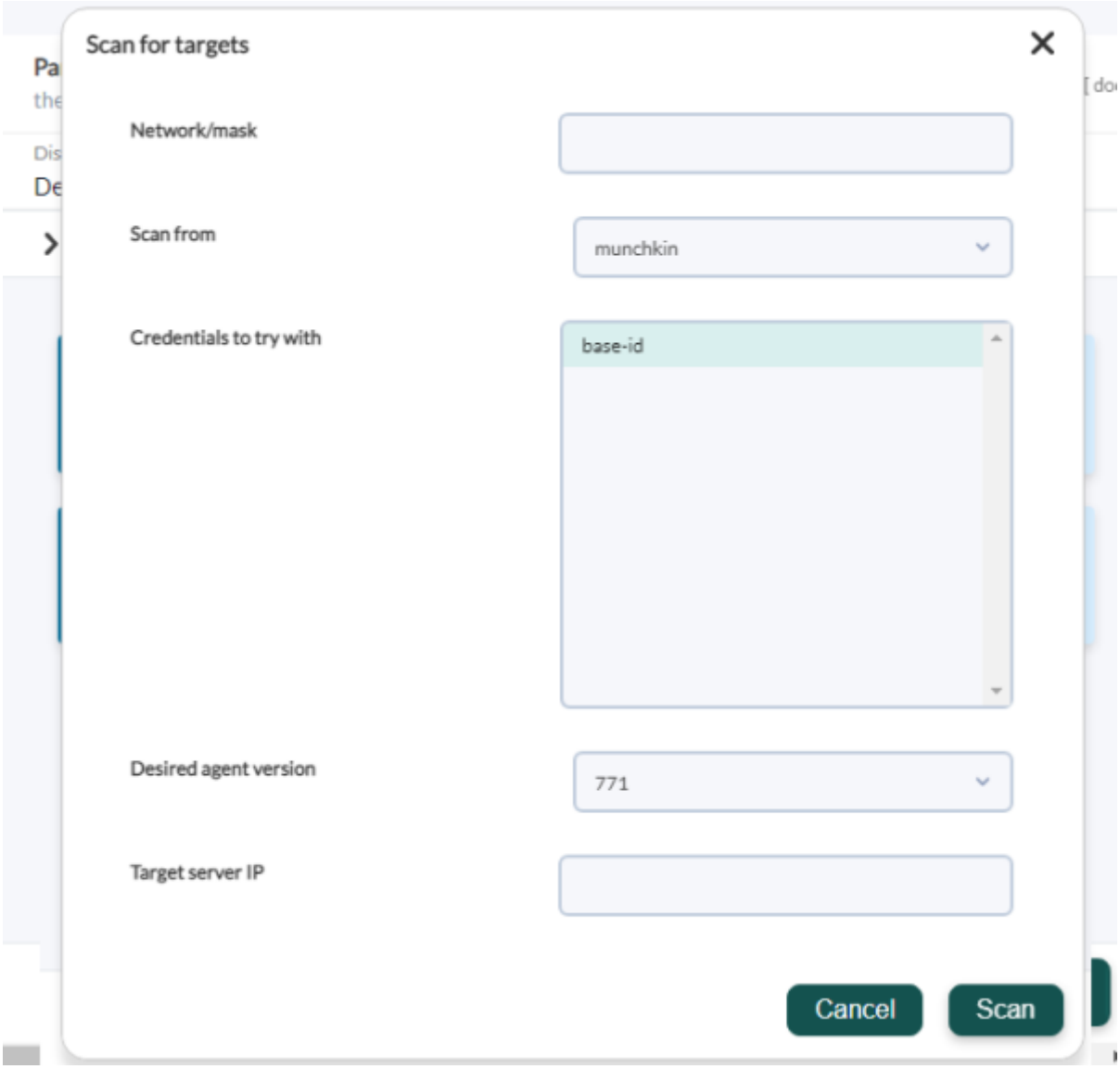
Поиск Целей

Цели развертывания

Для определения целей можно использовать любой из следующих параметров:

Сканирование одной или нескольких сетей в поисках целей.

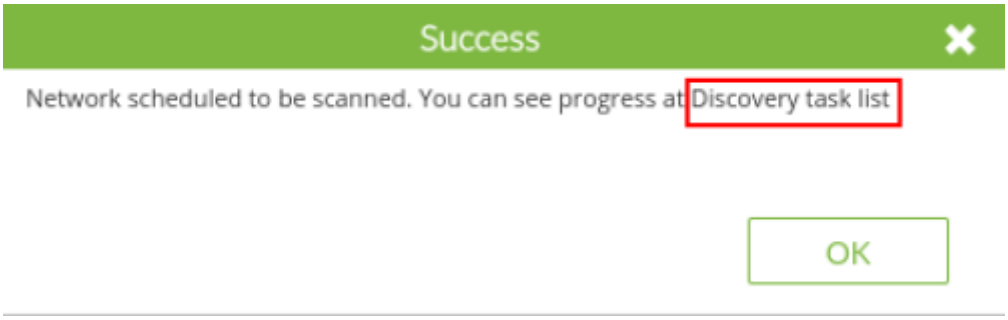
При нажатии кнопки сканировать цели появится всплывающее окно со следующими полями:



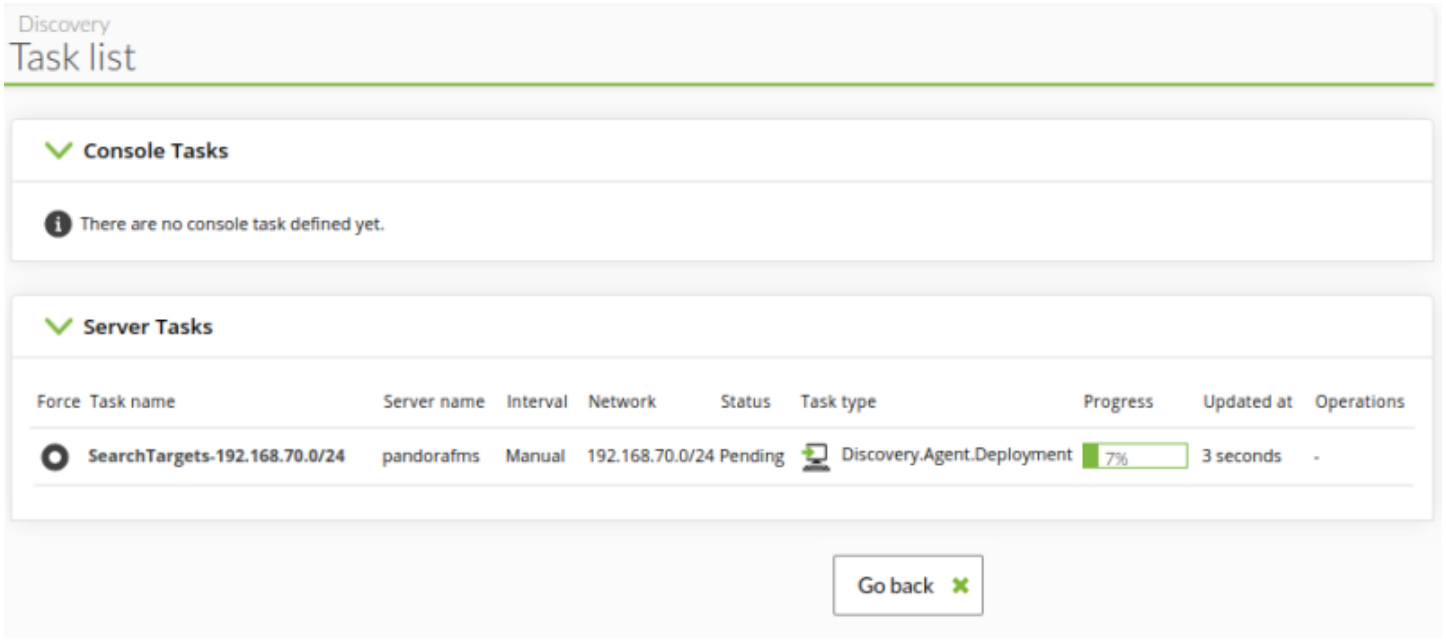
Вы должны указать:

- Network/mask: Сеть (или сети, разделенные запятыми) для сканирования.
- Scan from: Сервер Discovery, который будет выполнять сканирование.
- Credentials to try with: Учетные данные, которые будут использоваться для попыток подключения к обнаруженным целям.
- Desired agent version: Версия программного агента, зарегистрированная как *желательная* для обнаруженных целей.
- Target server IP: IP целевого сервера, на который будут указывать эти программные агенты при их установке (соответствует полю `server_ip` в файле конфигурации агента).

Когда вы нажмете 'Сканировать', вы получите подтверждение со ссылкой, по которой вы можете перейти, чтобы проверить ход выполнения этого задания.

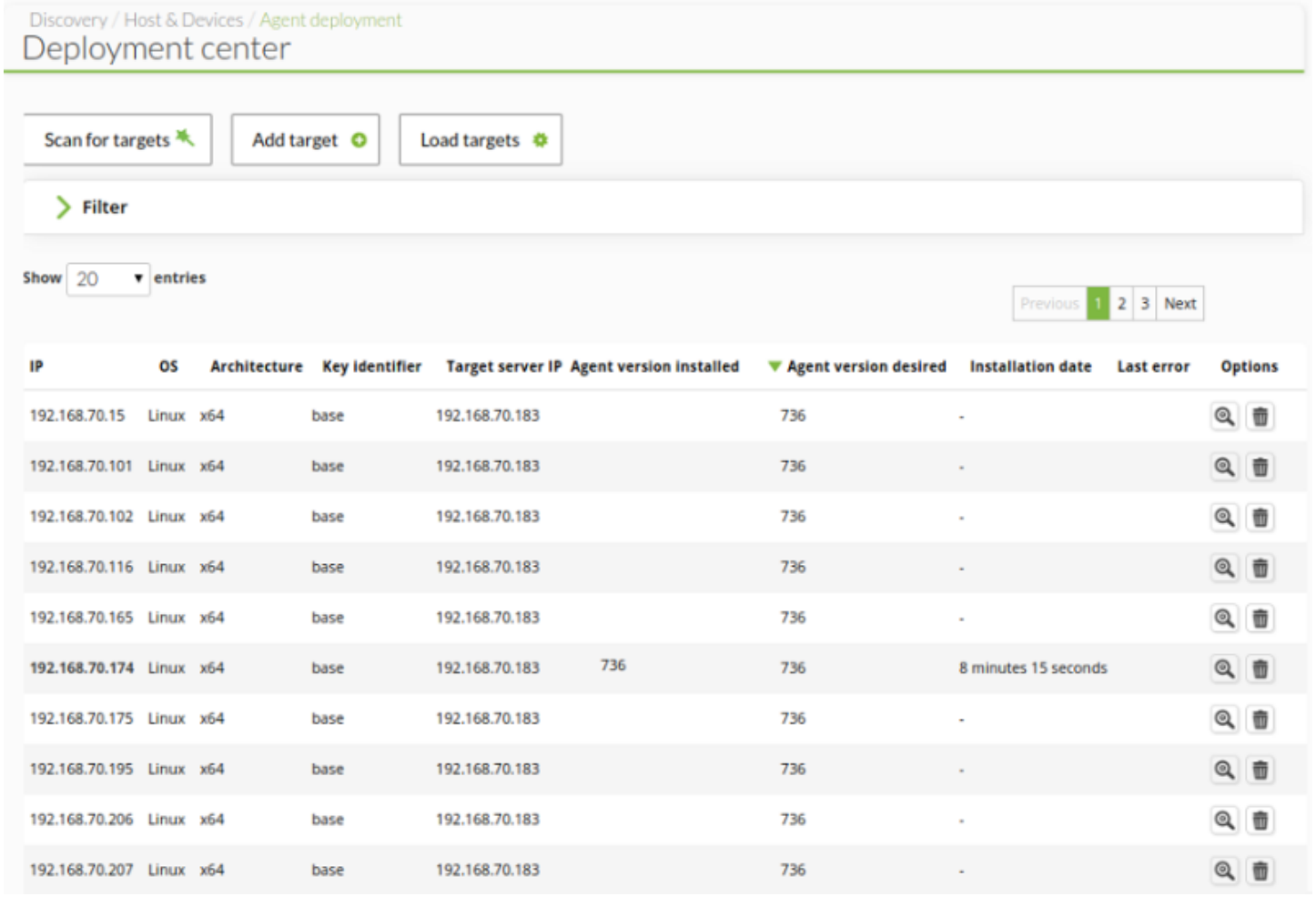


В списке задач появится новая запись:



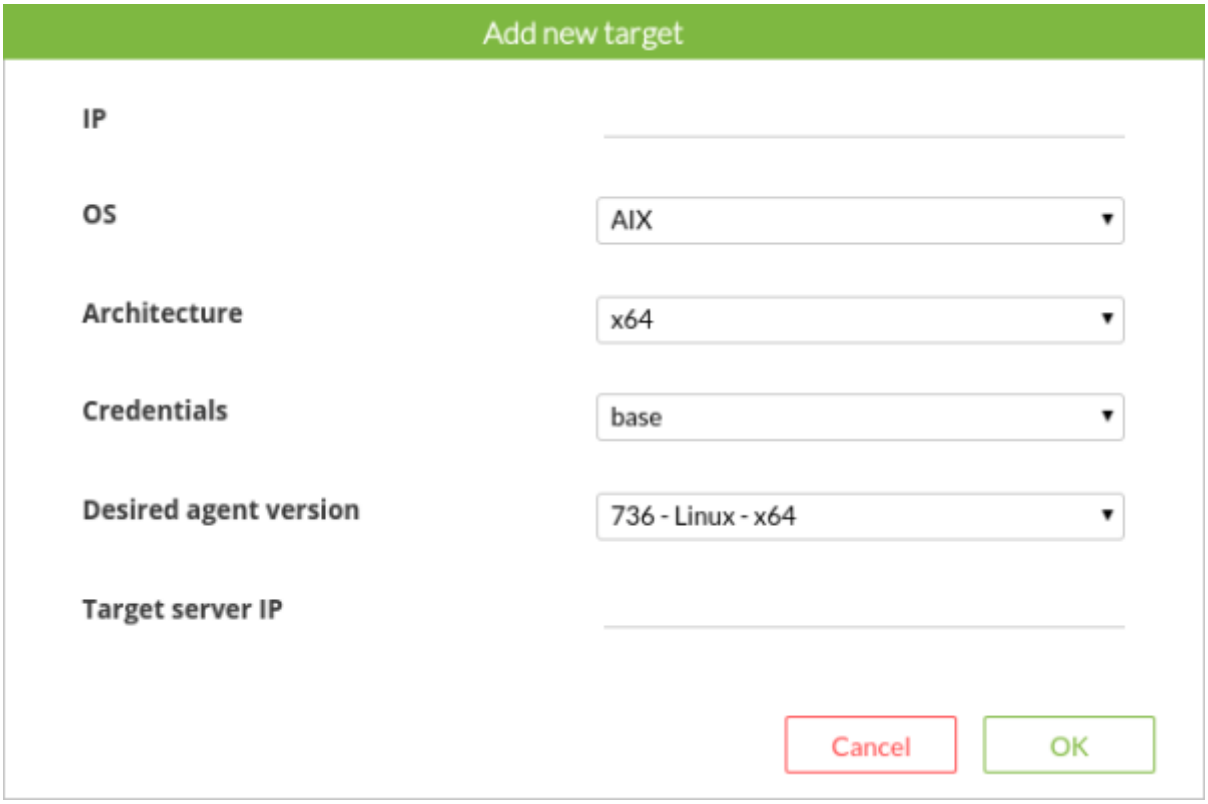
Задачи Discovery, связанные с развертыванием агента, являются волатильными задачами. После завершения они будут автоматически удалены. Информацию о сканировании или развертывании, успешном или неуспешном, можно просмотреть в самом центре развертывания.

По мере обнаружения возможных целей они будут появляться в центре развертывания:



Обнаруженные цели, добавленные в этот список, - это все найденные устройства, операционная система которых соответствует системам на базе Windows или Linux/Unix, независимо от того, были ли найдены действительные учетные данные или нет

Определение цели вручную



Вы можете вручную ввести цель, определив ее:

IP

IP-адрес или адреса для развертывания.

OS

Операционная система; в этой версии разрешены только Windows и системы на базе Linux/Unix, совместимые с инсталлятором `tar.gz` агента.

Architecture

Архитектура процессора, x86 (32-бит) или x64 (64-бит).

Credentials

Учетные данные, которые будут использоваться для подключения к цели.

Желаемая версия агента

Версия программного агента, который вы хотите развернуть.

Target server IP

IP-адрес сервера, на который будет указывать данный агент после установки (он соответствует полю `server_ip` в конфигурации программного агента).

Загрузите CSV-файл с информацией о целях

Если вы хотите записывать цели в массовом порядке, вы можете загрузить CSV-файл в следующем формате:

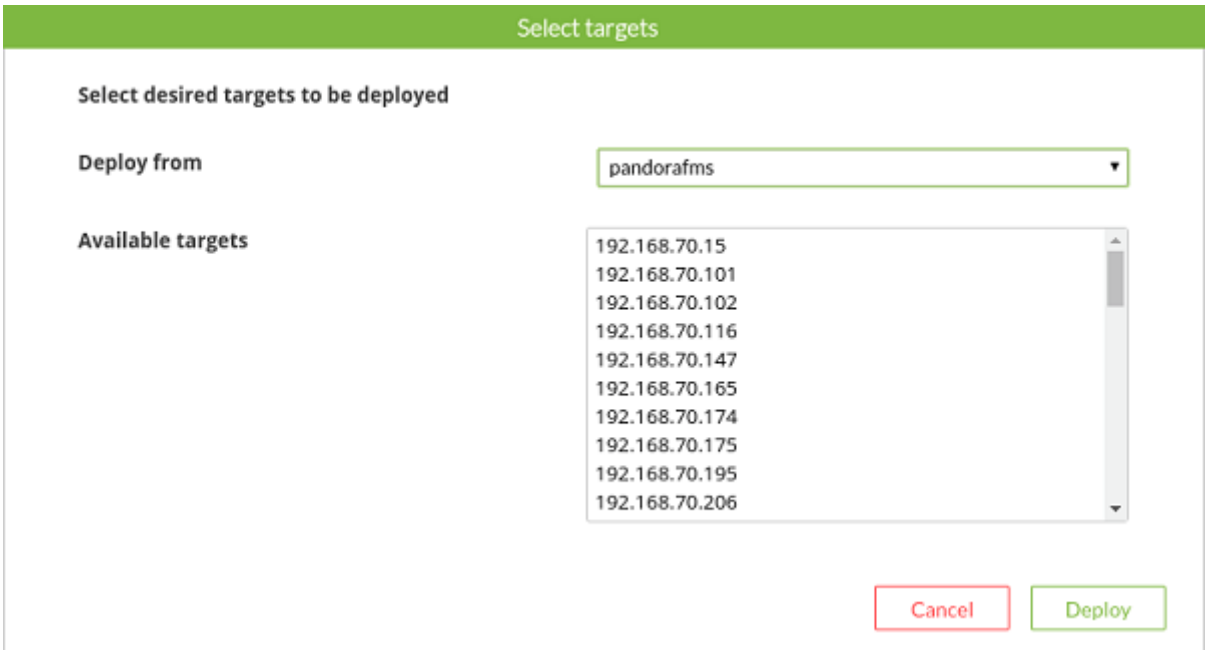
```
IP; OS; Architecture; Target agent version; Credential identifier; Target server ip
```

- IP: IP-адрес устройство, на котором установлен агент.
- Операционная система: поддерживаются AIX, BSD, HP-UX, Linux, Solaris, Windows.
- Архитектура: x64 или x86.
- Версия целевого агента: идентификационный номер агента, зарегистрированного в репозитории программных агентов.
- Идентификатор учетных данных: «Идентификатор» ключа, созданного в Хранилище учетных данных.
- IP целевого сервера: IP-адрес сервера, на который будет направлен развернутый программный агент.

Развертывание ПО

Вы можете запланировать развертывание только для тех целей, информация о которых является полной, с указанием учетных данных и версий программного обеспечения для развертывания.

Как только в списке появятся возможные цели, вы сможете запустить развертывание агента:

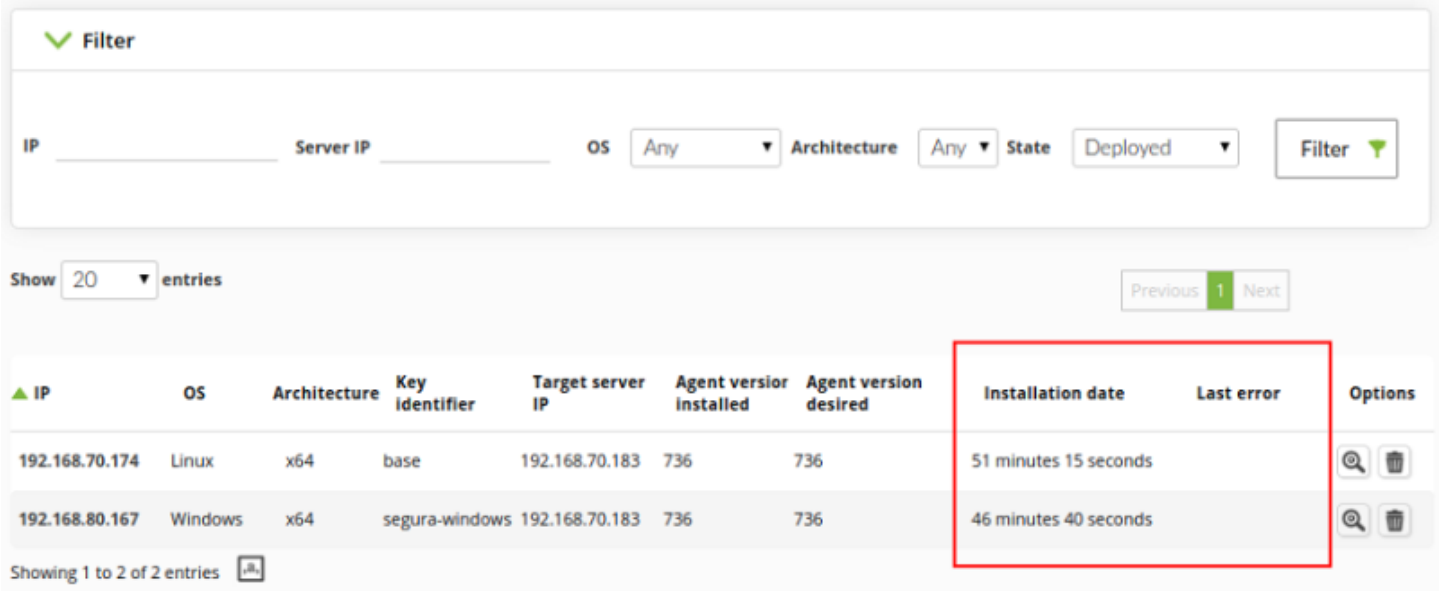


Выберите целевые IP из списка (появятся только действительные цели) и нажмите

развернуть.

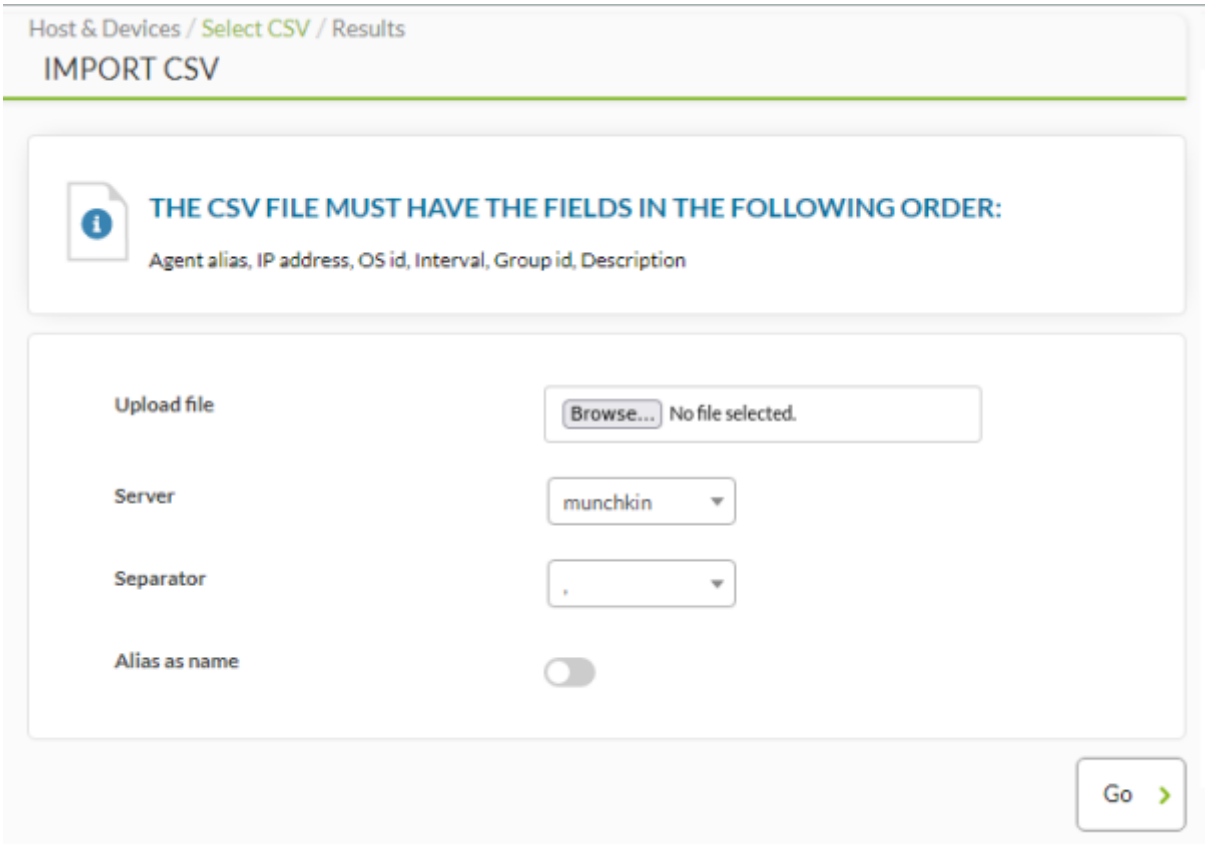
Автоматически для фонового развертывания создается задача Discovery, которая отвечает за установку агента на нужные цели.

Вы сможете подтвердить успешную установку агента из списка целей центра развертывания:



Имя цели также становится ссылкой на соответствующий агент Pandora FMS.

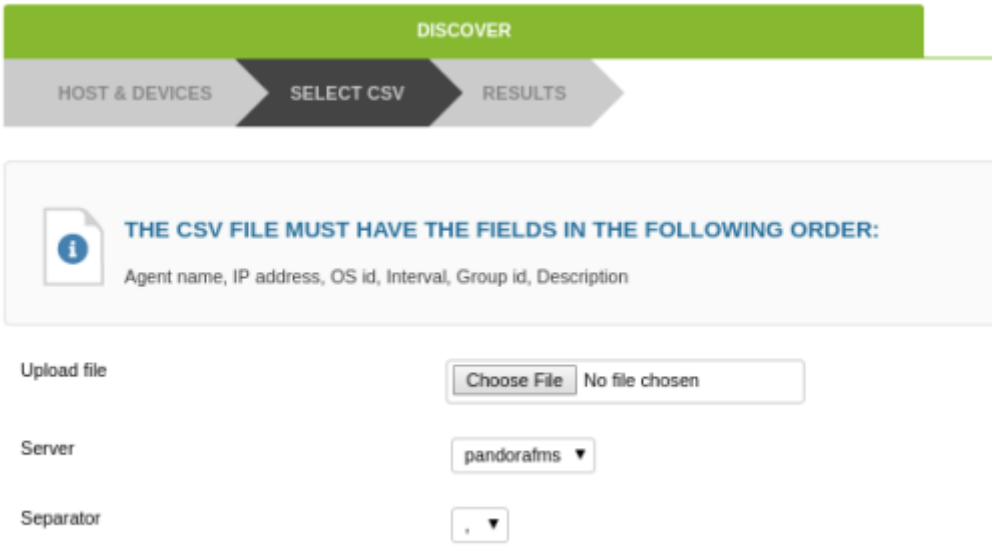
Пример ошибки: Пользователь не ввел не только IP-адрес цели, но и ее сетевую маску (достаточно IP-адреса). Когда система попытается развернуть программное обеспечение, она обнаружит, что формат IP неверен, и сообщит об этом пользователю:



Импортируйте список ваших устройств в CSV

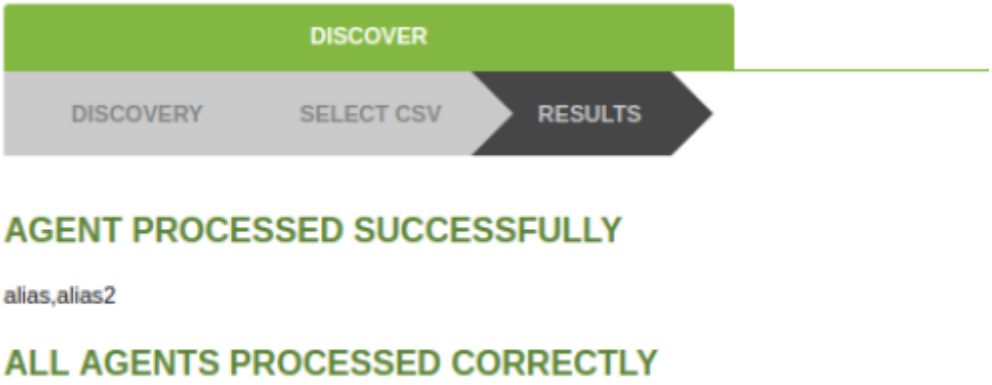
Вы можете импортировать список устройств для представления их в качестве агентов с помощью мастера импорта агентов через CSV.

Эта утилита только создает агентов в Pandora FMS для
ее удаленного мониторинга.



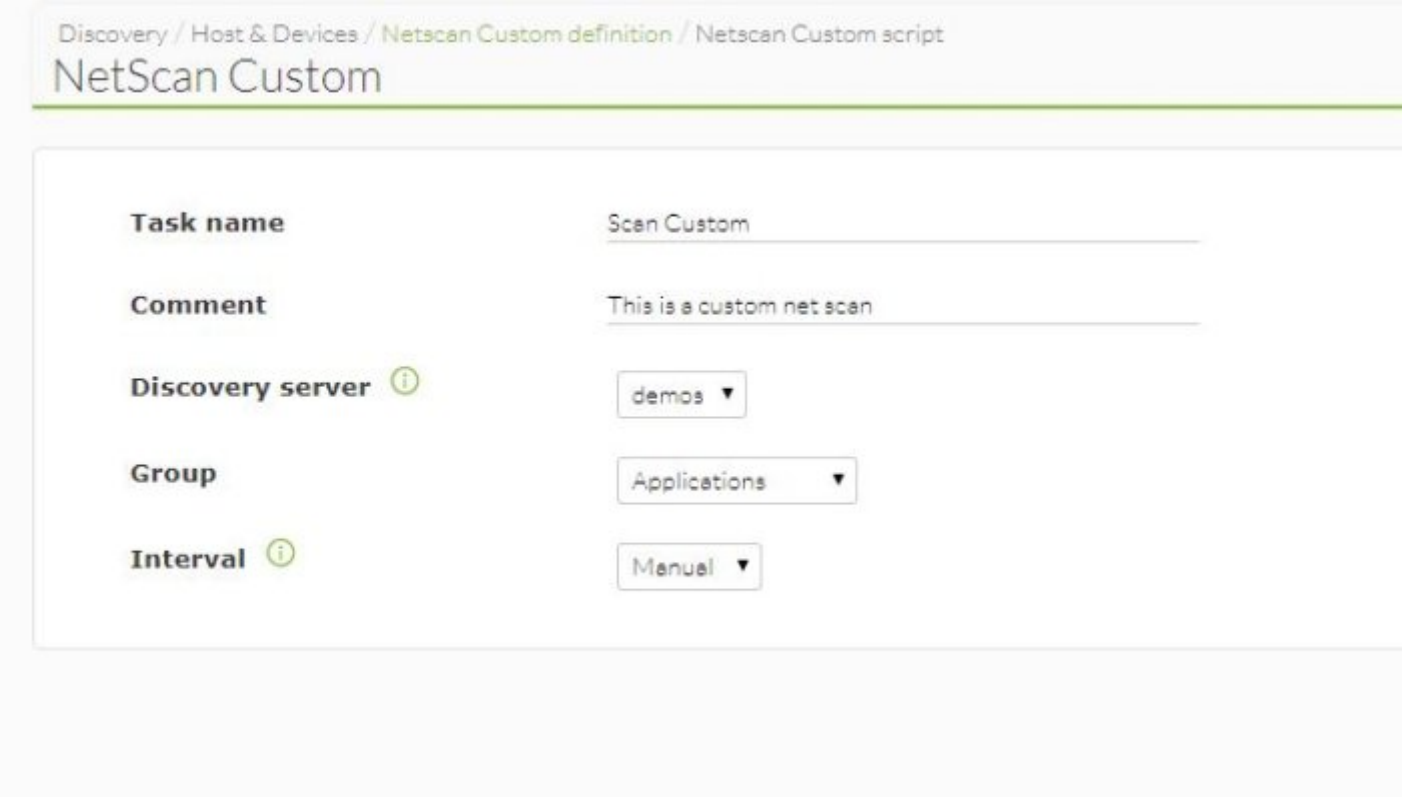
Вы должны выбрать используемый разделитель, сервер, на который вы хотите

импортировать, и файл, содержащий данные, затем нажмите *next*.



Custom NetScan

Позволяет выполнять пользовательские *скрипты* для выполнения задач распознавания сети.



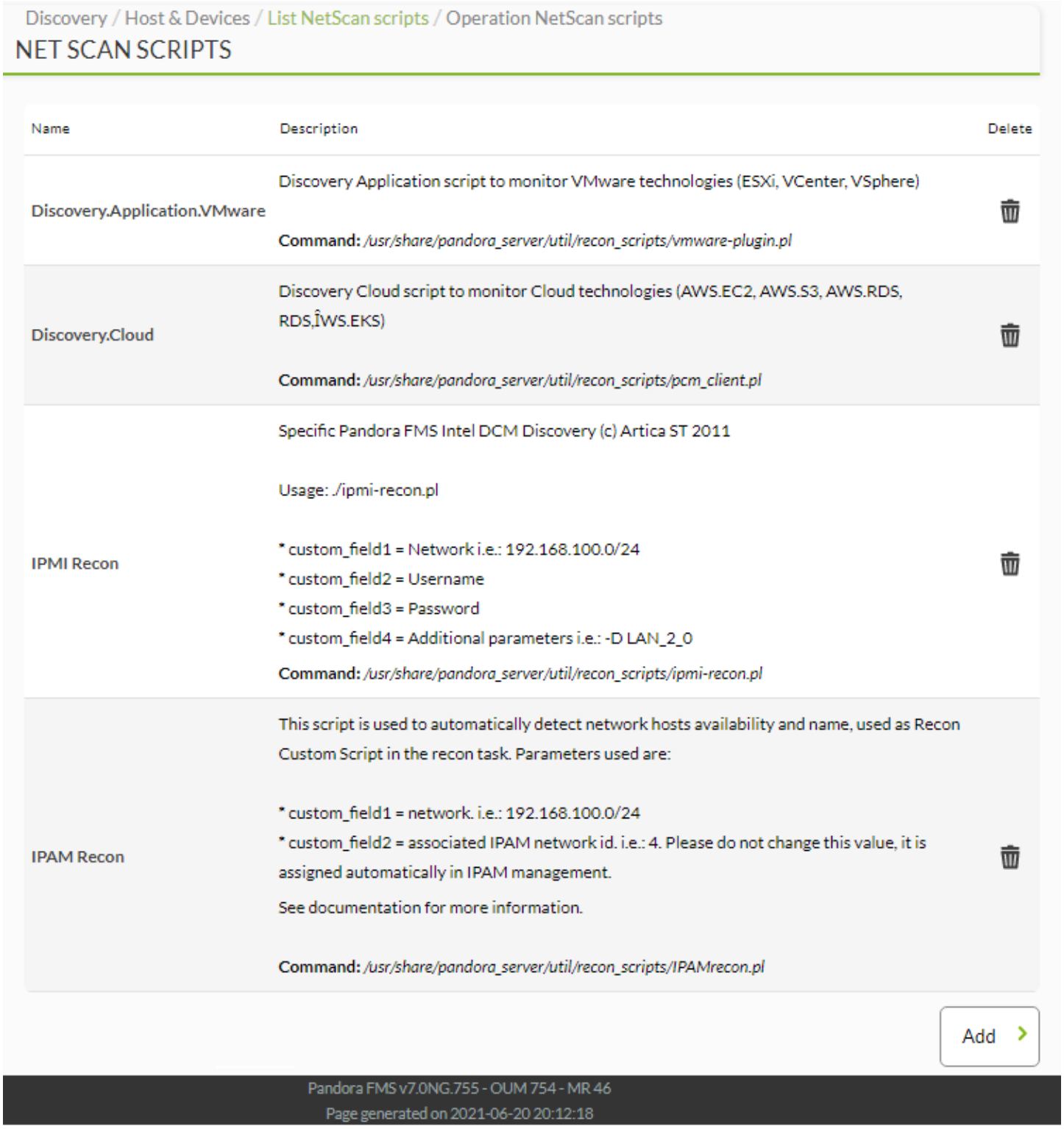
Укажите:

- Task name: Название задачи распознавания.
- Comment: Позволяет добавлять комментарии.
- Discovery server: Сервер, который будет выполнять задание.
- Group: Группа, к которой она принадлежит.
- Interval: Интервал выполнения.

После завершения процесса создания задания необходимо будет указать *скрипт*, который вы хотите запустить, а также конфигурационный файл, необходимый для его выполнения.

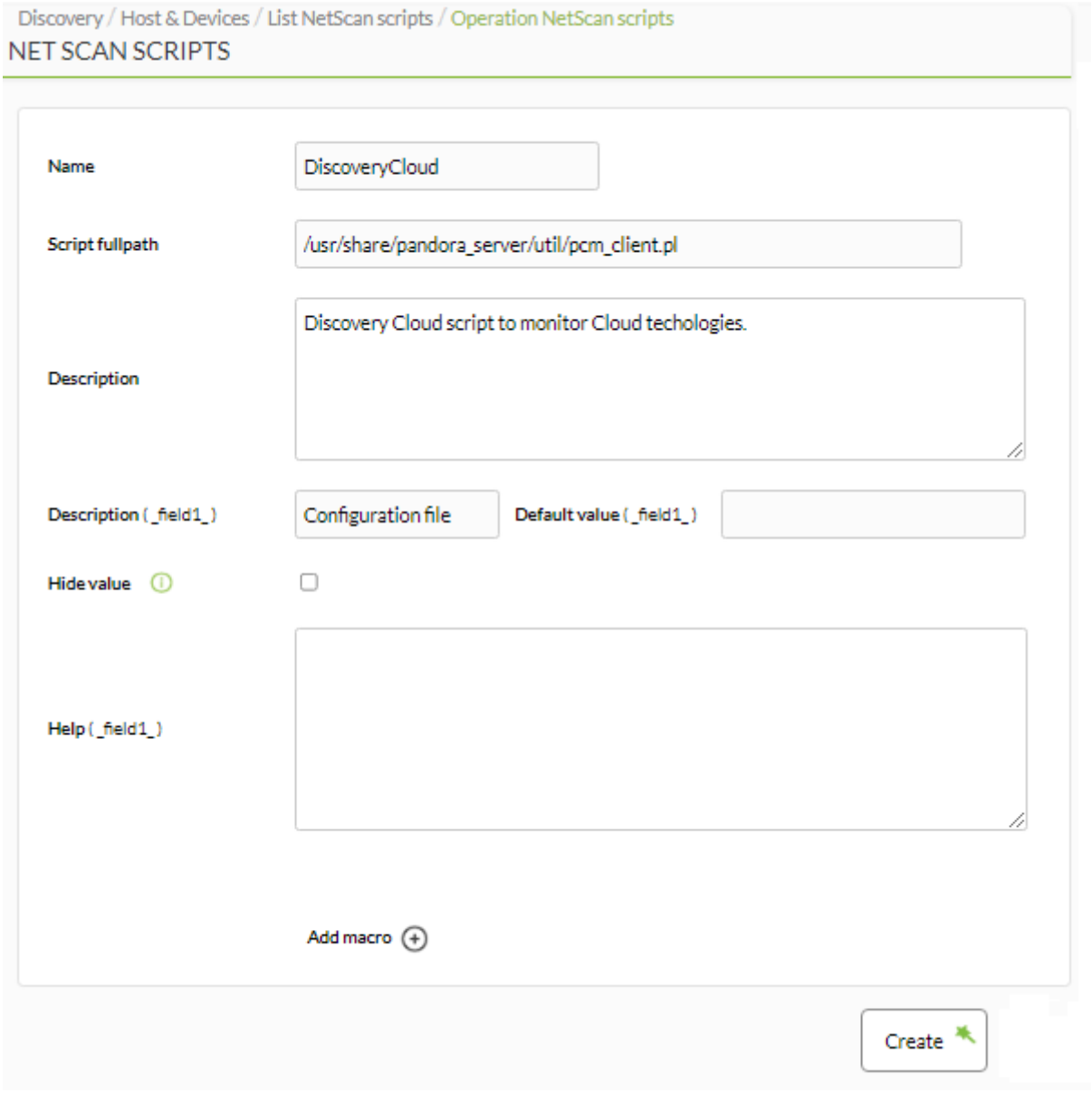
Net scan scripts

В этом разделе показаны различные *скрипты*, которые были созданы для выполнения пользовательских задач распознавания. Отображается вид, в котором задается название и описание задачи.



Pandora FMS позволяет добавлять дополнительные *скрипты* для облегчения мониторинга и распознавания необходимых сетей.

Параметры, которые должны быть определены:



- Name: Имя скрипта.
- Script fullpath: Путь, где находится скрипт.
- Description: Описание скрипта. Вы можете определить описания различных полей, а также значения по умолчанию для них.
- Hide value: Если вы хотите скрыть значение поля.
- Help: Поля справки.

Создание *скриптов* позволяет добавлять макросы для определения всех параметров, которые необходимы для правильного выполнения *скрипта*.

Вернуться в оглавление Pandora FMS