

Установка InfoWatch Crawler 6.11.4.52

Настройка базы данных
Задайте параметры подключения к базе данных Traffic Monitor

Тип базы данных

☐ Oracle ☒ PostgreSQL

IP-адрес или DNS-имя сервера базы данных Traffic Monitor: Порт: 5433

172.16.1.3

Имя базы данных Traffic Monitor (SID):

postgres

Имя пользователя:

iwtm

Пароль:

••••••••

Назад Далее Отмена

xxXX1234

Установка InfoWatch Crawler 6.11.4.52

Настройка Traffic Monitor
Задайте параметры подключения агента Consul

IP-адрес или DNS-имя сервера Traffic Monitor с установленным Consul:

172.16.1.3

Имя центра обработки данных, в котором работает Consul:

IWTM

Секретный ключ для шифрования сетевого трафика Consul:

Локальный IP адрес.
Это IP-адрес, который должен быть доступен всем остальным узлам кластера Consul:

172.16.1.4

Назад Далее Отмена

Чтобы узнать инфу про консул – ssh root@iwtm -> cat /opt/iw/tm5/etc/consul/consul.json

Имя ЦОДа – iwtm, ключ – encrypt

Установка InfoWatch Crawler 6.11.4.52

Настройка Traffic Monitor
Задайте параметры подключения к серверу Traffic Monitor

IP-адрес или DNS-имя сервера Traffic Monitor с установленным сервисом хранилища: Порт:

Токен плагина краулера для Traffic Monitor

Назад Далее Отмена

Токен брать на вебморде → Управление → плагины → IW Crawler

Установка InfoWatch Crawler 6.11.4.52

Установка сканера
Определите параметры учётной записи для сервиса сканера

Запись учётной службы сервиса сканера
☒ Локальная система ☐ Пользователь

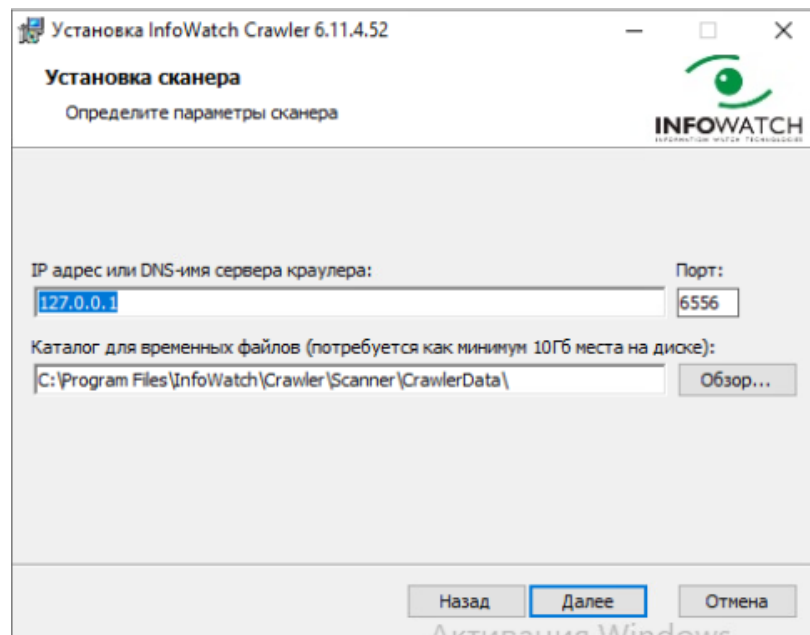
Имя пользователя:

Пароль:

Описание
Сервис будет запущен под учётной записью "Локальная система".

Назад Далее Отмена

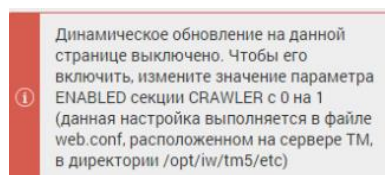
От локальной



Не трогать

Проверка – вебморда → краулер

Открыть Порты 6556 1337



ssh root@iwtm --> nano /opt/iw/tm5/etc/web.conf

```
{
  "consul": {
    "hostname": "127.0.0.1",
    "port": 8500,
    "token": "",
    "username": "consul_client"
  },
  "db": {
    "driver": "pgsql",
    "connstr": "driver=pgsql;localhost:port=5432;password=xxxx1234;schema=iwtm;username=iwtm_web",
    "debug": "",
    "hostname": null,
    "inlineTextDump": false,
    "kickers": {
      "agent": {
        "enabled": 1
      }
    },
    "blackboard": {
      "enabled": 1
    },
    "crawler": {
      "enabled": 0
    },
    "export": {
      "enabled": 1
    },
    "import": {
      "enabled": 1
    },
    "notifier": {
      "enabled": 1
    },
    "querytracker": {
      "enabled": 1
    }
  }
}
```

Недоступность Краулера в веб консоли InfoWatch Traffic Monitor

Описание проблемы: Краулер не доступен в веб консоли, имеется сообщение вида: "Нет работающих сканеров".

В протоколах InfoWatch Traffic Monitor могут фиксироваться сообщения вида:

```
2019/01/22 03:42:02 [error] [application] Can not get thrift: crawler 2019/01/22 03:42:02 [warning]
[crawler] crawler_not_found 2019/01/22 08:42:51 [error] [application] Can not get thrift: crawler
2019/01/22 08:42:51 [error] [exception.StringcodedException] StringcodedException: ThriftException in
/opt/iw/tm5/www/backend/protected/controllers/CrawlerController.php:321 Stack trace: #0
/opt/iw/tm5/www/backend/vendor/yiisoft/yii/framework/web/actions/CInlineAction.php(49):
CrawlerController->actionGetScanners() #1
/opt/iw/tm5/www/backend/vendor/yiisoft/yii/framework/web/CController.php(308): CInlineAction-
>runWithParams(Array) #2
/opt/iw/tm5/www/backend/vendor/yiisoft/yii/framework/web/filters/CFilterChain.php(133):
CController->runAction(Object(CInlineAction)) #3
/opt/iw/tm5/www/backend/protected/components/Controller.php(52): CFilterChain->run() #4
/opt/iw/tm5/www/backend/vendor/yiisoft/yii/framework/web/filters/CInlineFilter.php(58): Controller-
>filterInitLanguage(Object(CFilterChain)) #5
/opt/iw/tm5/www/backend/vendor/yiisoft/yii/framework/web/filters/CFilterChain.php(130):
CInlineFilter->filter(Object(CFilterChain)) #6
/opt/iw/tm5/www/backend/vendor/yiisoft/yii/framework/web/filters/CFilter.php(40): CFilterChain-
>run() #7 /opt/iw/tm5/www/backend/vendor/yiisoft/yii/framework/web/CController.php(1145):
CFilter->filter(Object(CFilterChain)) #8
/opt/iw/tm5/www/backend/vendor/yiisoft/yii/framework/web/filters/CInlineFilter.php(58):
CController->filterAccessControl(Object(CFilterChain)) #9
/opt/iw/tm5/www/backend/vendor/yiisoft/yii/framework/web/filters/CFilterChain.php(130):
CInlineFilter->filter(Object(CFilterChain)) #10
/opt/iw/tm5/www/backend/vendor/yiisoft/yii/framework/web/CController.php(291): CFilterChain-
>run() #11 /opt/iw/tm5/www/backend/vendor/yiisoft/yii/framework/web/CController.php(265):
CController->runActionWithFilters(Object(CInlineAction), Array) #12
/opt/iw/tm5/www/backend/vendor/yiisoft/yii/framework/web/CWebApplication.php(282):
CController->run('getScanners') #13
/opt/iw/tm5/www/backend/vendor/yiisoft/yii/framework/web/CWebApplication.php(141):
CWebApplication->runController('crawler/getScan...') #14
/opt/iw/tm5/www/backend/vendor/yiisoft/yii/framework/base/CApplication.php(185):
CWebApplication->processRequest() #15 /opt/iw/tm5/www/backend/index.php(24): CApplication-
>run() #16 {main} REQUEST_URI=/api/crawler/scanner HTTP_REFERER=https://10.10.10.22/crawler
```

3 Возможные решения:

- 1) Проверить работу служб сканера и сервера Краулера (должны быть запущены);
- 2) Выяснить имя сервера Краулера в настройках, которые можно найти в БД Infowatch Traffic Monitor в схеме iwtm, таблица crawler_servers, настройки хранятся в поле metadata, искать можно по слову name;
- 3) Проверить доступность портов Краулера Какие порты и протоколы нужны для работы InfoWatch Traffic Monitor и Device Monitor?

1 с сервера InfoWatch Traffic Monitor, например командой netcat:

```
nc -v crawler_server_name 6556
```

```
nc -v crawler_server_name 1337
```

При необходимости можно сделать:

- Если в DNS нет имени сервера Краулера и имя не определяется при проверке портов выше, то добавить его имя в файл /etc/hosts на сервере InfoWatch Traffic Monitor (с веб консолью);
- Если порты Краулера прослушиваются, но не доступны с сервера InfoWatch Traffic Monitor, то необходимо проверить работу фаерволов (встроенных или антивируса) или маршрутизации