

Лабораторная работа №3

« Конфигурирование и администрирование автоматизированной системы Infowatch Traffic Monitor 6 и Infowatch Device Monitor»

Цель работы – получение профессиональных компетенций по конфигурированию и администрированию автоматизированной системы IW TM 6 и модуля IW DM.

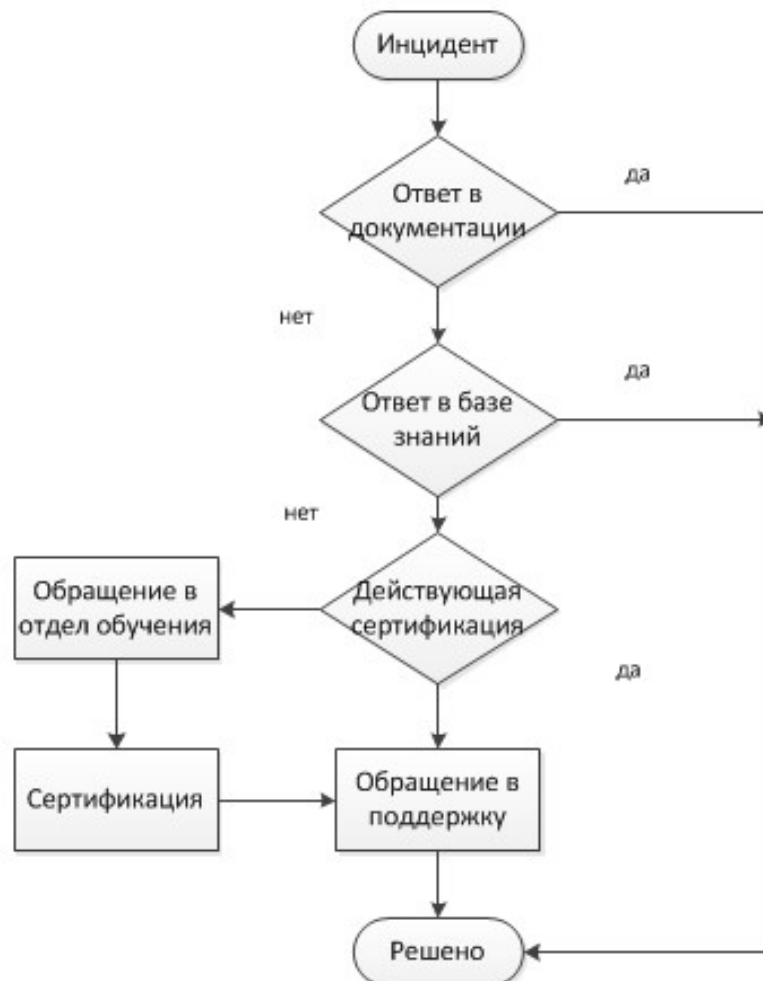
3.1 Основные сведения и команды необходимые для конфигурирования и администрирования системы.

Техническую поддержку конечного клиента оказывает компания-партнер или InfoWatch в зависимости от действующего договора на оказание услуг технической поддержки.

Для получения услуги технической поддержки следует обращаться по контактными данным предоставленным компанией-партнером или используя контактные данные технической поддержки InfoWatch: support@infowatch.com или +7(495) 22-900-22

Время работы технической поддержки компании InfoWatch: будние дни, с 7 до 21 по Московскому времени.

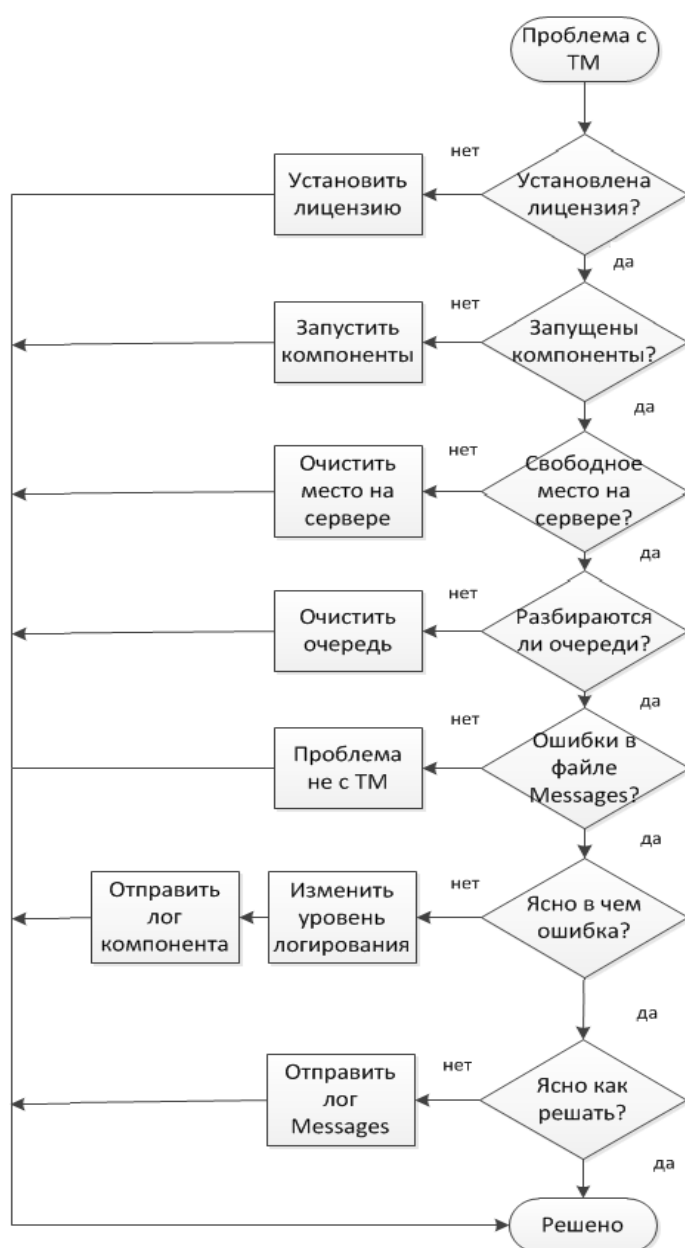
Алгоритм работы с технической поддержкой



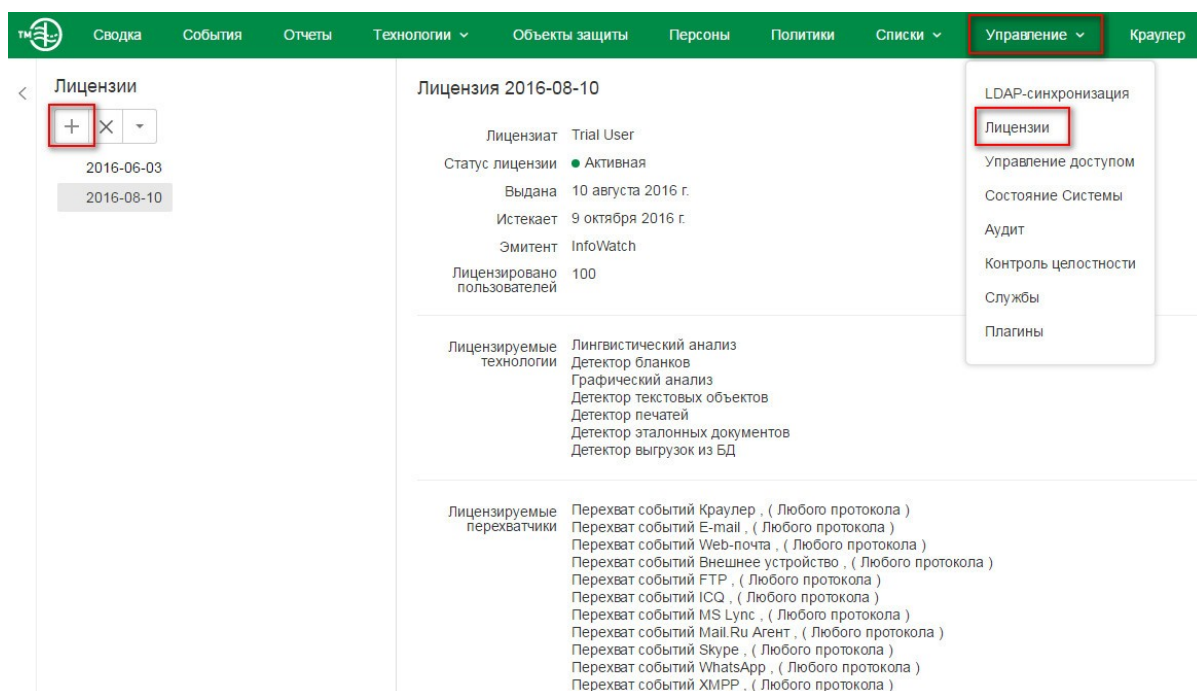
Рекомендации

Перед обращением в техническую поддержку необходимо ознакомиться с документацией по продукту и статьями базы знаний, чтобы удостовериться, что в нем нет решения вашей проблемы. В случае отсутствия данной информации, необходимо наиболее полно описать сложившуюся проблему, указав номер и описание возникшей ошибки, а также прикрепив к обращению скриншоты. По запросу от инженера InfoWatch необходимо предоставить диагностическую информацию. Методика сбора диагностической информации описана в разделе **“Как собрать детальную диагностическую информацию?”**.

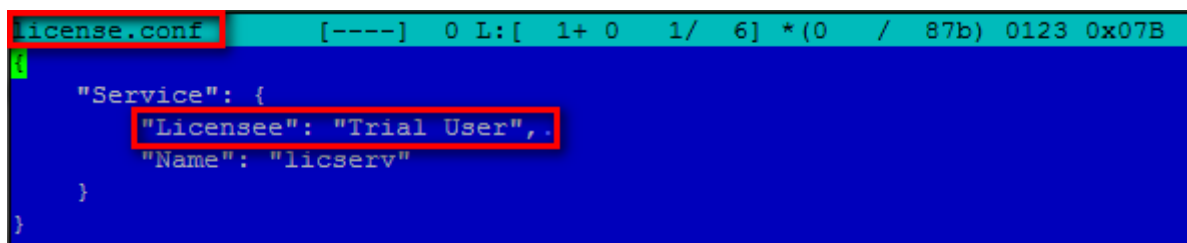
Алгоритм диагностики Traffic Monitor



Как загрузить лицензию InfoWatch Traffic Monitor?



- Загрузите файл лицензии через консоль управления Traffic Monitor, раздел Управление>Лицензии;
- войдите в интерпретатор командной строки сервера Traffic Monitor, например, с помощью SSH-клиента Putty;
- убедитесь, что параметр лицензиат, отображаемый в консоли, соответствует параметру Licensee в файле ***/opt/iw/tm5/etc/license.conf***



Лицензия 2016-08-10

Лицензиат	Trial User
Статус лицензии	● Активная
Выдана	10 августа 2016 г.
Истекает	9 октября 2016 г.
Эмитент	InfoWatch
Лицензировано пользователей	100

- перезапустите сервер Traffic Monitor следующей командой:

service iwtm restart

Как проверить статус/запустить компоненты InfoWatch Traffic Monitor?

Войдите в интерпретатор командной строки сервера Traffic Monitor и выполните необходимую команду.

service iwtm status (отобразить статус всех компонентов Traffic Monitor)

service iwtm start (запустить все компоненты Traffic Monitor)

service iwtm stop (остановить все компоненты Traffic Monitor)

service iwtm restart (перезапустить все компоненты Traffic Monitor)

service iwtm restart xapi_xapi (перезапустит только компонент xapi)

service iwtm stop cas (остановит только компонент cas)

Как проверить и очистить место на сервере InfoWatch Traffic Monitor?

Для проверки свободного места на сервере Traffic Monitor подключитесь к серверу с помощью SSH-клиента и выполните следующую команду:

df -h

Для очистки места на сервере Traffic Monitor вы можете удалить:

- Дистрибутив системы из директории **/opt/distr/**

rm -rf /opt/distr/ (удаление дистрибутивов Traffic Monitor)

- Информацию из временной директории Traffic Monitor:

service iwtm stop (остановка сервера Traffic Monitor)

rm -rf /opt/iw/tm5/tmp/* (удаление временных файлов Traffic Monitor)

service iwtm start (запуск сервера Traffic Monitor)

- Лог-файлы (с расширением .gz) в директории **/var/log**

rm -rf /var/log/infowatch/*.gz (удаление лог-файлов Traffic Monitor с расширением gz)

Примечание: также рекомендуется проверить и в случае необходимости обработать объекты в очередях Traffic Monitor.

С более детальной информацией об очистке места можно ознакомиться в статье Базы Знаний **“Очистка InfoWatch Traffic Monitor от временных файлов”**.

Как проверить и очистить очередь на сервере InfoWatch Traffic Monitor?

Очереди событий хранятся в каталоге **/opt/iw/tm5/queue/**. Войдите в интерпретатор командной строки сервера Traffic Monitor под пользователем **iwtm** и запустите скрипт **iw_qtool** для ознакомления с доступными опциями:

su – iwtm (смена пользователя на iwtm)

./bin/iw_qtool (запуск скрипта iw_qtool)

./bin/iw_qtool stat /opt/iw/tm5/queue/db/ (отображение актуальной информации о количестве событий в очереди загрузки в базу данных)

./bin/iw_qtool erase /opt/iw/tm5/queue/errors/ (удаление событий из очереди ошибок)

./bin/iw_qtool move /opt/iw/tm5/queue/errors/ /opt/iw/tm5/queue/db/
(перемещение объектов из очереди ошибок в очередь загрузки в базу данных)

Как настроить OCR-экстрактор ABBY?

1. Отредактируйте значения полей SerNum и Pwd в конфигурационном файле **/opt/iw/tm5/etc/image2text_fre.conf** следующим образом:
"SerNum": ""
"Pwd": ""
2. Скачать файл с лицензией
3. Скопировать файл с лицензией в директорию **/var/lib/ABBY/SDK/11/Licenses/**
4. Предоставить пользователю **iwtm** права на доступ к файлу: **chown iwtm:iwtm /var/lib/ABBY/SDK/11/Licenses/XXXXXX.LocalLicense**
5. Перезапустить сервис **warpd**: **service iwtm restart warpd**

Как открыть файл с логом InfoWatch Traffic Monitor?

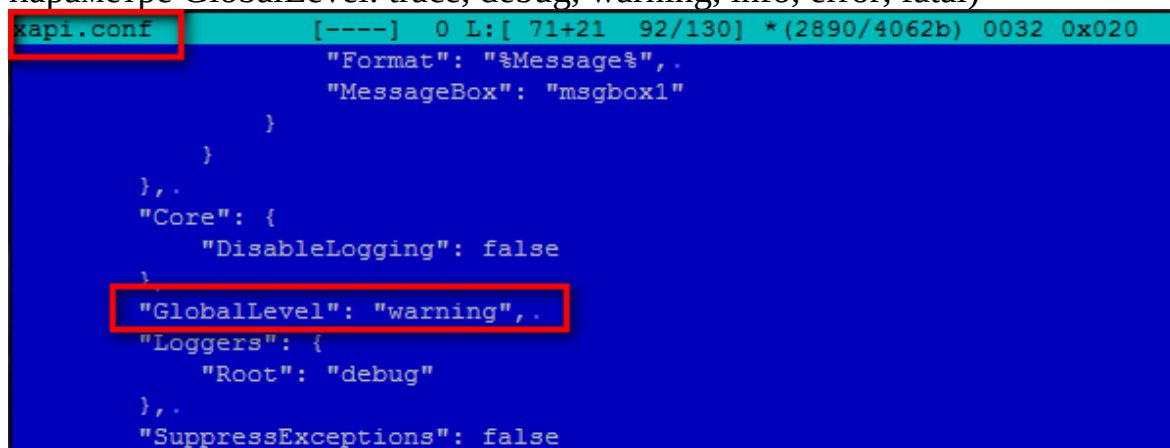
Войдите в интерпретатор командной строки сервера Traffic Monitor и выполните следующую команду:

```
# tail -f /var/log/messages
```

Как изменить уровень логирования компонента InfoWatch Traffic Monitor?

Откройте конфигурационный файл Traffic Monitor

mcedit /opt/iw/tm5/etc/xapi.conf (изменение уровня логирования для xapi в параметре GlobalLevel: trace, debug, warning, info, error, fatal)



```
xapi.conf [----] 0 L: [ 71+21 92/130] *(2890/4062b) 0032 0x020
    "Format": "%Message%",
    "MessageBox": "msgbox1"
  }
},
  "Core": {
    "DisableLogging": false
  },
  "GlobalLevel": "warning",
  "Loggers": {
    "Root": "debug"
  },
  "SuppressExceptions": false
```

Для того чтобы изменения вступили в действие, перезапустите сервис Traffic Monitor

```
# service iwtm restart xapi_xapi
```

Примечание: не забудьте вернуть компонент к уровню по умолчанию (3), после устранения инцидента для сохранения места на жестком диске.

Как открыть файл с логом компонента InfoWatch Traffic Monitor?

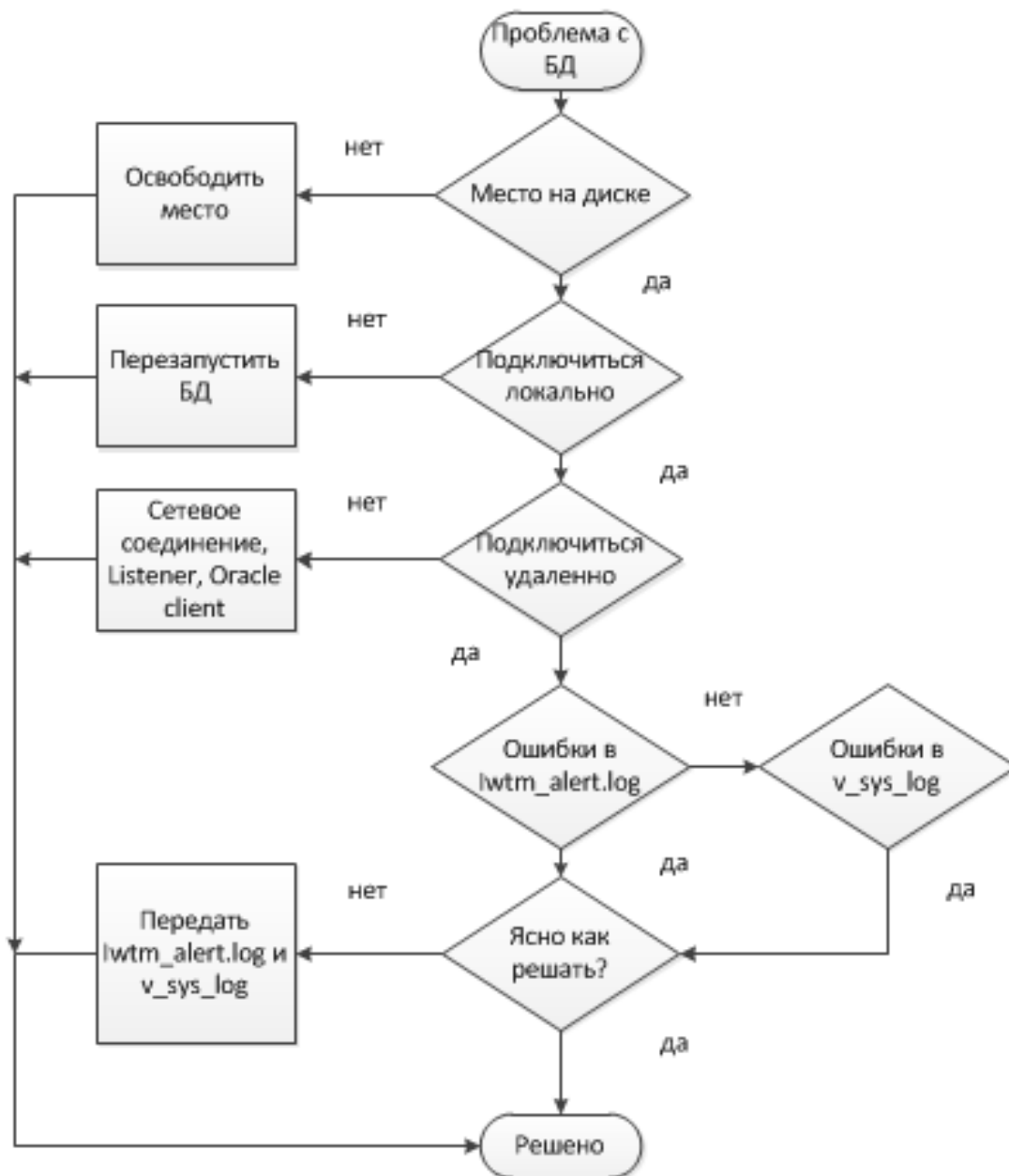
Файл с логами компонентов Traffic Monitor находится в директории **/var/log/Infowatch**.

Для того чтобы открыть файл с логом компонента *xapi*, необходимо выполнить следующую команду:

```
# tail -f /var/log/Infowatch/xapi.log
```

Для того чтобы открыть файл с логом компонента *serman*, необходимо выполнить следующую команду: **# tail -f /var/log/Infowatch/serman.log**

Алгоритм диагностики базы данных



Как проверить и очистить место на диске Базы Данных?

Для проверки свободного места на сервере Базы Данных подключитесь к серверу с Базой Данных с помощью SSH-клиента и выполните следующую команду:

df -h

Oracle Database

/opt/iw/tm5/bin/dbtools/dbconf-iwdrop-oracle set violation100

(установка глубины хранения для объектов с нарушениями)

/opt/iw/tm5/bin/dbtools/dbconf-iwdrop-oracle set noviolation 50

(установка глубины хранения для объектов без нарушений)

/opt/iw/tm5/bin/dbtools/dbconf-iwdrop-oracle set other 50

(установка глубины хранения для объектов со скриншотами)

/opt/iw/tm5/bin/dbtools/dbconf-iwdrop-oracle enable violation

(включение автоматического выполнения задания Oracle)

/opt/iw/tm5/bin/dbtools/dbconf-iwdrop-oracle enable noviolation

(включение автоматического выполнения задания Oracle)

/opt/iw/tm5/bin/dbtools/dbconf-iwdrop-oracle enable other

(включение автоматического выполнения задания Oracle)

Для того чтобы запустить удаление более старых табличных пространств вручную, необходимо выполнить следующую команду:

**# /opt/iw/tm5/bin/dbtools/dbconf-iwdrop-oracle start
IWTM_DELETE_TABLESPACES**

Также рекомендуем ознакомиться со статьей использование “**Удаление ежедневных табличных пространств**”. В данной статье описан процесс использования процедуры IWDRDP базы данных Oracle.

Для настройки автоматической подрезки логов базы данных alert_iwtm.log рекомендуем ознакомиться со статьей “**Настройка logrotate для протокола alert_iwtm.log**”.

PostgreSQL Database

/opt/iw/tm5/bin/dbtools/dbconf-iwdrop-postgres.sh set violation 100

(установка глубины хранения для объектов с нарушениями)

/opt/iw/tm5/bin/dbtools/dbconf-iwdrop-postgres.sh set noviolation 50

(установка глубины хранения без нарушений)

/opt/iw/tm5/bin/dbtools/dbconf-iwdrop-postgres.sh set other 50

(установка глубины хранения со скриншотами)

/opt/iw/tm5/bin/dbtools/dbconf-iwdrop-postgres.sh enable violation

(включение автоматического выполнения задания PostgreSQL)

/opt/iw/tm5/bin/dbtools/dbconf-iwdrop-postgres.sh enable noviolation

(включение автоматического выполнения задания PostgreSQL)

/opt/iw/tm5/bin/dbtools/dbconf-iwdrop-postgres.sh enable other

(включение автоматического выполнения задания PostgreSQL)

Как проверить, запущена ли база данных Oracle?

Oracle Database

su – oracle (смена пользователя на oracle)

sqlplus iwtm/xxXX1234@iwtm (подключение к базе данных iwtm под пользователем iwtm)

SQL>select * from version; (запрос в базу данных)

PostgreSQL Database

su – postgres (смена пользователя на postgres)

psql –d postgres (подключение к базе данных Postgres под пользователем postgres)

select * from “pg_tables”; (запрос в базу данных по списку таблиц)

\q (выход из СУБД)

Как остановить/запустить базу данных?

Oracle Database

su – oracle (смена пользователя на oracle)

wsqlplus / as sysdba (подключение к базе данных под администратором)

SQL> shutdown immediate (выключение базы данных Oracle)

su – oracle (смена пользователя на oracle)

wsqlplus / as sysdba (подключение к базе данных под администратором)

SQL> startup (запуск базы данных Oracle)

PostgreSQL Database

service postgresql-9.4 stop (выключение базы данных PostgreSQL)

service postgresql-9.4 start (запуск базы данных PostgreSQL database)

Как проверить принимает ли База Данных подключения извне?

Oracle Database

su – oracle (смена пользователя на oracle)

lsnrctl status (проверка статуса Listener).

Если в результатах выполнения команды есть следующие строки, то база данных может принимать подключения извне, в противном случае listener необходимо запустить.

```
Services Summary...
Service "iwtm" has 2 instance(s).
  Instance "iwtm", status UNKNOWN, has 1 handler(s) for this service...
  Instance "iwtm", status READY, has 2 handler(s) for this service...
```

Для запуска Listener выполните следующую команду:

su – oracle (смена пользователя на oracle)

lsnrctl start (запуск Listener)

Как получить логи Базы Данных?

Oracle Database

Для получения полной информации о состоянии базы данных, откройте файл **alert_iwtm.log**, находящийся в каталоге **/u01/app/oracle/diag/rdbms/iwtm/iwtm/trace/**.

mcview /var/log/alert_iwtm.log (основная информация о состоянии базы данных)

Диагностическая информация о работе Базы Данных содержится в таблице **v_sys_log**. Сбор диагностической информации подробно описан в статье базы знаний “**SQLDeveloper сбор диагностической информации**” из раздела “**Полезные статьи базы знаний**”.

PostgreSQL Database

mcview /u01/postgres/pg_log/postgres.log (основная информация о состоянии базы данных)

Полезные советы по устранению неполадок

Как проверить что объекты получены сервером Traffic Monitor?

tcpdump -i eth0 port 4101 (проверка теневых копий с Device Monitor)

tcpdump -i eth0 port 1344 (проверка объектов с Proxu сервера)

tcpdump -i eth0 port 25 or port 80 or port 5190 (проверка поступления трафика (SMTP, HTTP, ICQ) с сетевого оборудования)

tcpdump -i eth0 port 25 (проверка объектов с почтового сервера)

Как перезапустить frontend?

service php-fpm restart && service nginx restart && service redis restart
(перезагружает компоненты ответственные за отображение web-консоли)

Как собрать детальную диагностическую информацию о системе?

Тип проблемы	Алгоритм сбора информации
База данных	<ul style="list-style-type: none">Для предоставления полной информации о состоянии базы данных, передайте в поддержку файл alert_iwtm.log, находящийся в каталоге /var/log/Или соберите диагностическую информацию из таблицы v_sys_log, используя статью базы знаний “SQLDeveloper сбор диагностической информации” из раздела “Полезные статьи базы знаний”.
Traffic Monitor	<ul style="list-style-type: none">Для проверки состояния компонентов Traffic Monitor, подключитесь к серверу Traffic Monitor и выполните следующую команду: # service iwtm statusОбщая диагностическая информация о работоспособности компонентов Traffic Monitor хранится в файле /var/log/messages. Для того чтобы вывести ее на экран, можно воспользоваться командой: # tail -f /var/log/messages

	<p>Сообщения типа [Fatal], [Error], [Warning], содержат описание неисправности.</p> <ul style="list-style-type: none"> • Диагностическая информация по отдельным компонентам Traffic Monitor 6 хранится в директории <i>/var/log/Infowatch/</i>. Для того, чтобы собрать более детальную информацию о работе того или иного компонента, измените уровень логирования компонента в соответствующем конфигурационном файле (параметр <i>GlobalLevel = Debug</i>), перезапустите компонент командой и откройте соответствующий файл: <p style="text-align: center;"><i># service iwtm restart имя_компоненты</i></p> <p style="text-align: center;"><i># tail -f /var/log/Infowatch/имя_компоненты.log</i></p>
Сервер Device Monitor	<p>Общая информация о неисправности сервера DM хранится в логе приложения Windows, на котором установлен сервер DM.</p> <p>Для того, чтобы открыть лог приложений, перейдите в Пуск>Панель управления>Администрирование>Просмотр событий>Журналы Windows>Приложения</p> <p>Для получения более детальной информации необходимо включить режим расширенного логирования, используя статью “Включение расширенного режима логирования сервера DM” из раздела “Полезные статьи базы знаний”</p>
Агент Device Monitor	<p>Детальную информацию о состоянии агента Device Monitor можно получить в консоли Device Monitor. В консоли Device Monitor перейдите в секцию “Рабочие станции” и выберете необходимую рабочую станцию.</p> <p>Вызовете контекстное меню, перейдите в меню Диагностика и выберете опцию «Включить».</p> <p>После того как диагностическая информация собрана, выключите сбор данных в меню Диагностика и сохраните файл, нажав «Передать».</p> <p>На рабочей станции с агентом Device Monitor детальная информация о состоянии агента Device Monitor хранится в следующей директории:</p> <p style="text-align: center;"><i>C:\Program Files\InfoWatch\DeviceMonitor\Client\Logs\</i></p>

База знаний. Полезные статьи

1. SQLDeveloper сбор диагностической информации:
<https://kb.infowatch.com/pages/viewpage.action?pageId=34963459>
2. Включение расширенного режима логирования сервера DM:
<https://kb.infowatch.com/pages/viewpage.action?pageId=32408343>
3. Изменение параметров протоколирования Агента InfoWatch Device Monitor утилитой rmtlogctr
<https://kb.infowatch.com/pages/viewpage.action?pageId=16515524>
4. Очистка InfoWatch traffic Monitor от временных файлов:
<https://kb.infowatch.com/pages/viewpage.action?pageId=16515365>
5. Удаление ежедневных табличных пространств <https://kb.infowatch.com/pages/viewpage.action?pageId=9666757>
6. Настройка logrotate для протокола alert_iwtm.log:
<https://kb.infowatch.com/pages/viewpage.action?pageId=16515473>

3.2. Содержание технологических этапов выполнения работы.

1. Установка лицензии IW ТМ 6.
2. Включение-выключение компонент IW ТМ 6 в конфигурационном файле cas.conf (разбор назначения компонент с тренером).
3. Настройка OCR (рассмотрение с тренером).
4. Устранение неисправностей (рассмотрение с тренером):
 - чистка места (дистрибутивы, лог файлы, очереди);
 - настройка уровня логирования;
 - работа с базой данных Oracle Database, PostgreSQL Database (чистка места, проверка подключения, настройка сбора логов);
 - другие неисправности.
5. Сбор детальной диагностической информации о системе.

3.3. Вопросы и ответы

1. Как записаться на обучение?

Обратиться к менеджеру InfoWatch по телефону: +7(495) 22-900-22

2. Как продлить лицензию?

Обратиться в техническую поддержку по почте support@infowatch.com или по телефону +7(495) 22-900-22

3. Как получить доступ в базу знаний?

Перейти на kb.infowatch.com и ввести полученные логин и пароль.

4. Как получить доступ к коммерческому portalу?

Перейти на cp.infowatch.com и ввести полученные логин и пароль.

5. Где можно найти более детальную информацию о процессе внедрения решения?

cp.infowatch.com

6. Где можно найти шаблоны документов, необходимых для внедрения?

cp.infowatch.com

7. Где можно скачать документация по продуктам Infowatch?

kb.infowatch.com

8. Что делать, если срок действия сертификации истекает?

После истечения сертификация техническая поддержка будет вправе отказывать вам в услугах. Для продления сертификации обратитесь к менеджеру Infowatch для записи на обучение.