InfoWatch Activity Monitor 1.0.0 Руководство по установке

12/04/2021

© АО “ИнфоВотч”

Тел./Факс +7 (495) 229-00-22

http://www.infowatch.ru

СОДЕРЖАНИЕ

1 Аудитория 4

2 Комплект документов 5

3 Техническая поддержка пользователей 6

4 Типы установки, аппаратное и программное обеспечение 7

5 Как установить InfoWatch Activity Monitor 13

5.1 Настройка сетевых правил доступа 16

5.2 Описание файла лицензии 16

5.3 Устранение неполадок и восстановление Системы 18

6 Как обновить InfoWatch Activity Monitor 19

7 Как удалить InfoWatch Activity Monitor 20

8 Установка Device Monitor (DM) 21

Настоящее руководство содержит сведения по установке и удалению InfoWatch Activity Monitor – программного обеспечения, предназначенного для контроля деятельности сотрудников.

1 Аудитория

Информация, содержащаяся в Руководстве, предназначена для пользователей, работающих с Системой (выполняющих настройку конфигурации, анализ информационных объектов и т. п.).

Руководство рассчитано на пользователей, знакомых с основами работы в среде операционной системы Linux.

2 Комплект документов

В комплект документации по InfoWatch Activity Monitor входят:

- «InfoWatch Activity Monitor. Руководство по установке». Содержит описание процесса установки, обновления и удаления Activity Monitor.
- «InfoWatch Activity Monitor. Руководство администратора». Содержит информацию по настройке и подготовке к работе Activity Monitor.
- «InfoWatch Activity Monitor. Руководство пользователя». Содержит описание порядка работы и решения задач в Activity Monitor.

3 Техническая поддержка пользователей

При возникновении проблем и вопросов, связанных с работой Системы, вы можете обратиться в службу технической поддержки:

- компании InfoWatch по адресу support@infowatch.com, если продукт приобретен напрямую у InfoWatch;
- партнера компании InfoWatch, если продукт приобретен у партнера компании InfoWatch.

Часы работы Службы технической поддержки – с 7:00 до 21:00 по московскому времени с понедельника по пятницу, исключая официальные выходные и праздничные дни в РФ. Вы также можете посетить раздел технической поддержки на нашем сайте: www.infowatch.ru/services/support.

Перед обращением в службу технической поддержки рекомендуется посетить раздел База знаний на сайте: https://kb.infowatch.com/. Возможно, он уже содержит ответ на ваш вопрос или решение возникшей ситуации.

4 Типы установки, аппаратное и программное обеспечение

Activity Monitor (далее – Система) имеет 2 варианта установки и размещения относительно сервера Traffic Monitor (далее – TM):

- на выделенном сервере для работы с одним или несколькими серверами TM (stand-alone);
- возможна установка на одном сервере с TM. Данный тип установки не рекомендуется ввиду повышенной нагрузки на аппаратные средства.

Примечание:

Поддерживается синхронизация Системы с TM начиная с версии 6.10.10.

Важно!

Для корректной работы Системы версия DM должна быть не ниже 7.0.X.

Рекомендуется использовать TM и DM одинаковой или близких версий. Подробнее о совместимости см. в статье Базы знаний InfoWatch "Особенности совместимости разных версий TM, DM и Агентов".

Доступны несколько вариантов установки Системы относительно InfoWatch Vision (далее – Vision):

- Установка Системы на отдельный сервер;
- Установка Системы к уже имеющемуся Vision.

Важно!

Перед установкой Системы к уже имеющемуся Vision, необходимо обновить Vision до версии 2.2.2.

Система не может быть установлена совместно с Vision версии 2.3.X.

Минимальные системные требования к объему оперативной памяти и жесткого диска, необходимые для установки продукта:

RAM	HDD	Процессор
2 GB	30 GB	Количество ядер – 3

Нагрузка на аппаратное обеспечение, требуемое для эксплуатации продукта, рассчитывается на основе объема анализируемых данных и числа одновременно работающих с Системой пользователей:

Общее количество сотрудников в организации	Количество Офицеров безопасности	Срок хранения событий	Аппаратное обеспечение (для процессора разрядностью 64 bit, с поддержкой инструкций SSE 4.2)			
			RAM	HDD	Процессор	Рекомендуемая спецификация сервера
До 100	1	3 месяца	4 GB	800 GB	Количество ядер – 4 Частота – 3.1 ГГц	Количество ядер – 4 Частота – 3 ГГц RAM 8 GB HDD 4 TB
До 500	1		10 GB	4 TB	Количество ядер – 4 Частота – 3.1 ГГц	Количество ядер – 4 Частота – 3 ГГц RAM 16 GB HDD 4 TB
До 1000	2		16 GB	8 TB	Количество ядер – 8 Частота – 3.1 ГГц	Количество ядер – 8 Частота – 3 ГГц RAM 16 GB HDD 40 TB
До 10000	20		128 GB	72 TB для томов ClickHouse рекомендуется использовать SSD-диски	Количество ядер – 32 Частота – 3.5 ГГц	Количество ядер – 32 Частота – 3 ГГц RAM 128 GB HDD 400 TB

Важно!

Существует ограничение, касающееся скорости HDD. Минимальная скорость равна 50 IOPS (количество последовательных операций ввода-вывода в секунду) для HDD с 7200 оборотов в минуту.

При первоначальной загрузке данных в Систему нагрузка на HDD возрастает, поэтому может потребоваться скорость 500 IOPS. При дальнейшей периодической синхронизации нагрузка уменьшается.

Система может быть установлена на следующие операционные системы:

- Astra Linux Special Edition 1.6 "Смоленск";
- Red Hat Enterprise Linux 7.5 и более поздние;
- CentOS Linux 7 и более поздние.

В качестве СУБД используется PostgreSQL 12.

Работа Офицера безопасности поддерживается в браузерах Google Chrome и Яндекс.Браузер.

> **Важно!**
>
> Систему рекомендуется устанавливать в организациях, где количество пользователей Active Directory не превышает 100000.

Как установить Систему дополнительно к Vision:

Совместная установка с Vision:

Если необходимо установить Систему в дополнение к уже имеющемуся Vision, выполните действия, описанные в инструкции ниже.

Дистрибутив продукта представляет собой архив iw_am_setup_1.0.0.xxx.tar.xz**,** где xxx — номер сборки. Архив содержит набор бинарных модулей образов контейнеров, необходимых для развертывания продукта без доступа к сети Интернет (offline-установка). Архив также содержит программу установки. Программа установки написана на языке Python версии 2.7. Для установки продукта в целевой ОС может потребоваться установка интерпретатора этого языка. Пакет с интерпретатором не входит в состав дистрибутива продукта.

> **Важно!**
>
> Для корректной работы используемого Системой Docker 19.03 в окружении CentOS и Red Hat Enterprise Linux 7 обновите политики SELinux. Для этого скачайте и установите пакет `container-selinux-2.107-1.el7_6.noarch.rpm`. Данный пакет не входит в состав дистрибутива продукта.

> **Важно!**
>
> Перед установкой продукта настройте правила POD сети или отключите межсетевой экран (подробнее см. "Конфликты при взаимодействии firewalld и Kubernetes", "Полное отключение межсетевого экрана"). В противном случае после установки продукт может быть неработоспособен.

Чтобы установить Систему:

1. Создайте целевую директорию на диске, например, activity_monitor:
   `mkdir activity_monitor`
2. Скопируйте архив **iw_am_setup_1.0.0.xxx.tar.xz** в созданную директорию.
3. Распакуйте архив с дистрибутивом продукта в эту директорию:
   `tar xf iw_am_setup_1.0.0.xxx.tar.xz`

Примечание:

Чтобы установить продукт на ОС CentOS 7, может потребоваться пакет **xz-utils**. Данный пакет содержит инструменты командной строки для работы с форматом сжатия **xz**. Проверьте наличие пакета **xz-utils** или установите его, затем выполните следующие команды:

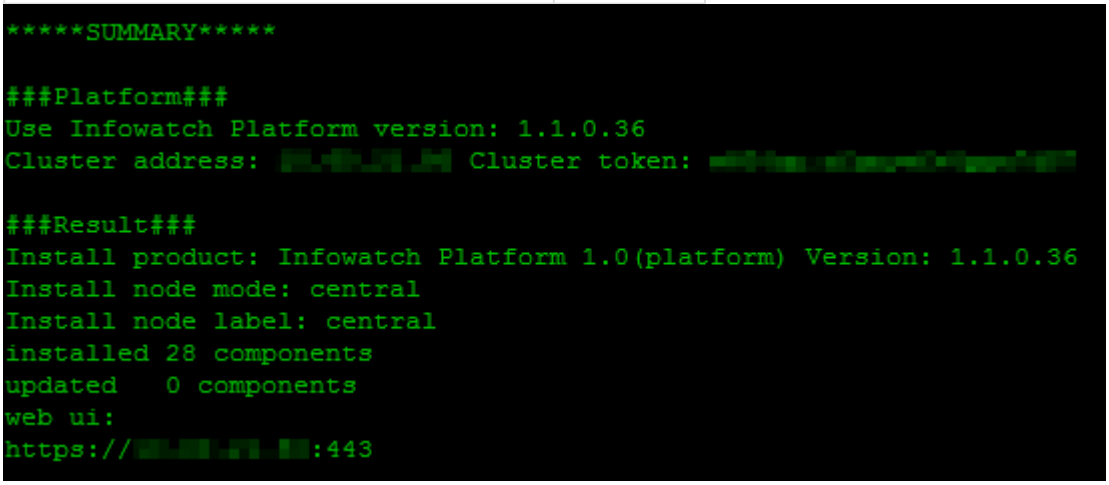
a. Распаковать архив и получить tar-файл:
   `unxz iw_am_setup_1.0.0.xxx.tar.xz`
b. Распаковать полученный tar-файл в текущую директорию:
   `tar -xvf iw_am_setup_1.0.0.xxx.tar`

4. Перейдите в подпапку **platform** и введите команду `/setup.py update`
5. Вернитесь в папку **activity monitor** и запустите программу интерактивной установки продукта:
   `./setup.py install`
6. Дождитесь окончания процесса установки. Программа установит компоненты продукта и требуемое окружение.
7. Убедитесь, что сервисы в списке ниже запустились, выполнив команду `kubectl get pods -n infowatch`

Список сервисов:

Сервис	Статус
clickhouse-central-db8687699-bfgxv	Running
cluster-agent-ppxkf	Running
cluster-central-767f5fb6cb-ttjrr	Running
comment-central-7d5cb49896-htd58	Running
configstorage-central-774c89b976-b5ld7	Running
datacollector-central-8548d67f96-m5cpp	Running
datastorage-central-67945bd764-vjwkw	Running
department-central-87494fbd9-tsnks	Running
dicsyncdrvldap-central-77b954c7b6-4clrs	Running
dicsyncdrvtm-central-c86f66446-bxvpb	Running
dictionary-central-568748b6b6-fkvg9	Running
dossier-central-658b467fbd-n44tl	Running
epevents-central-798cbbb698-jgr2w	Running
factsldrtm-central-bfb9d5d56-z9cbw	Running

Сервис	Статус
factsstorage-central-6ff5c5588c-5w9c4	Running
graph-central-8848897db-s9rjp	Running
guard-central-57b55ffb6b-ld5s7	Running
guiapps-central-d57cfb5bb-tsq9w	Running
intcoordinator-central-56cc6848df-z67p2	Running
license-central-57dfd89f77-2q625	Running
pmagent-central-55785969cb-xz8fs	Running
pobjects-central-6b5b446d6-2jqgh	Running
policy-central-74fcfbf78d-486cz	Running
postgresql-central-769c7945b7-bnsfw	Running
profile-central-665dd6977-b258q	Running
queryfacade-central-74bbd477d5-64zkp	Running
refscatalog-central-6996ff7544-lrgkx	Running
structure-central-76d7c74cf6-jkv98	Running
tarantool-central-54b8977f-k84wh	Running
taskscheduler-central-6b9b9fff45-cskq9	Running
tusker-central-c698699bd-b47zk	Running
webgui-central-84fcc4b476-p8jdc	Running



8. Введите в браузере полученный IP-adress, чтобы начать использование Системы. Подробнее о сервисах Clickhouse, Tarantool, PostgreSQL, Datastorage см. "Глоссарий".

См. также:

- Настройка сетевых правил доступа
- Описание файла лицензии
- Устранение неполадок и восстановление Системы

5 Как установить InfoWatch Activity Monitor

Установка продукта InfoWatch Activity Monitor (далее — Система) производится вручную, с помощью командной строки.

Дистрибутив продукта представляет собой архив iw_am_setup_1.0.0.xxx.tar.xz**,** где xxx — номер сборки. Архив содержит набор бинарных модулей образов контейнеров, необходимых для развертывания продукта без доступа к сети Интернет (offline-установка). Архив также содержит программу установки. Программа установки написана на языке Python версии 2.7. Для установки продукта в целевой ОС может потребоваться установка интерпретатора этого языка. Пакет с интерпретатором не входит в состав дистрибутива продукта.

Важно!

Для корректной работы используемого Системой Docker 19.03 в окружении CentOS и Red Hat Enterprise Linux 7 обновите политики SELinux. Для этого скачайте и установите пакет `container-selinux-2.107-1.el7_6.noarch.rpm`. Данный пакет не входит в состав дистрибутива продукта.

Важно!

Перед установкой продукта настройте правила POD сети или отключите межсетевой экран (подробнее см. "Конфликты при взаимодействии firewalld и Kubernetes", "Полное отключение межсетевого экрана"). В противном случае после установки продукт может быть неработоспособен.

Чтобы установить Систему:

1. Создайте целевую директорию на диске, например, activity_monitor:
   `mkdir activity_monitor`
2. Скопируйте архив **iw_am_setup_1.0.0.xxx.tar.xz** в созданную директорию.
3. Распакуйте архив с дистрибутивом продукта в эту директорию:
   `tar xf iw_am_setup_1.0.0.xxx.tar.xz`

   Примечание:

   Чтобы установить продукт на ОС CentOS 7, может потребоваться пакет **xz-utils**. Данный пакет содержит инструменты командной строки для работы с форматом сжатия **xz**. Проверьте наличие пакета **xz-utils** или установите его, затем выполните следующие команды:
   a. Распаковать архив и получить tar-файл:
      `unxz iw_am_setup_1.0.0.xxx.tar.xz`
   b. Распаковать полученный tar-файл в текущую директорию:
      `tar -xvf iw_am_setup_1.0.0.xxx.tar`
4. Запустите программу интерактивной установки продукта:
   `./setup.py install`
5. Ознакомьтесь с условиями лицензионного соглашения. Оно содержит несколько страниц. Для перехода на следующую страницу используйте клавишу **Enter**.

6. Введите "**y**", чтобы принять лицензионное соглашение, и нажмите **Enter**.
7. Выделите объем оперативной памяти для размещения данных Clickhouse (по умолчанию 80%) и нажмите **Enter**.
8. Укажите путь для размещения данных Clickhouse (по умолчанию `/mnt/chdata`) и нажмите **Enter**.
9. Выделите объем дискового пространства для размещения данных Clickhouse (по умолчанию 30%) и нажмите **Enter**.
10. Укажите путь для размещения данных Tarantool (по умолчанию `/mnt/trdata`) и нажмите **Enter**.
11. Выделите объем дискового пространства для `/mnt/trdata` (по умолчанию 200MB) и нажмите **Enter**.
12. Укажите путь для размещения данных PostgreSQL (по умолчанию `/mnt/pgdata`) и нажмите **Enter**.
13. Выделите объем дискового пространства для `/mnt/pgdata` (по умолчанию 30%) и нажмите **Enter**.
14. Укажите путь для хранения данных (по умолчанию `/mnt/dsdata`) и нажмите **Enter**.
15. Выделите объем дискового пространства для `/mnt/dsdata (`по умолчанию 30%`)` и нажмите **Enter**.
16. Укажите порт подключения к веб-интерфейсу (по умолчанию `443`) и нажмите **Enter**.
17. Дождитесь окончания процесса установки. Программа установит компоненты продукта и требуемое окружение.
18. Убедитесь, что сервисы в списке ниже запустились, выполнив команду `kubectl get pods -n infowatch`
    Список сервисов:

Сервис	Статус
clickhouse-central-db8687699-bfgxv	Running
cluster-agent-ppxkf	Running
cluster-central-767f5fb6cb-ttjrr	Running
comment-central-7d5cb49896-htd58	Running
configstorage-central-774c89b976-b5ld7	Running
datacollector-central-8548d67f96-m5cpp	Running
datastorage-central-67945bd764-vjwkw	Running
department-central-87494fbd9-tsnks	Running
dicsyncdrvldap-central-77b954c7b6-4clrs	Running
dicsyncdrvtm-central-c86f66446-bxvpb	Running
dictionary-central-568748b6b6-fkvg9	Running
dossier-central-658b467fbd-n44tl	Running
epevents-central-798cbbb698-jgr2w	Running

factsldrtm-central-bfb9d5d56-z9cbw	Running
factsstorage-central-6ff5c5588c-5w9c4	Running
graph-central-8848897db-s9rjp	Running
guard-central-57b55ffb6b-ld5s7	Running
guiapps-central-d57cfb5bb-tsq9w	Running
intcoordinator-central-56cc6848df-z67p2	Running
license-central-57dfd89f77-2q625	Running
pmagent-central-55785969cb-xz8fs	Running
pobjects-central-6b5b446d6-2jqgh	Running
policy-central-74fcfbf78d-486cz	Running
postgresql-central-769c7945b7-bnsfw	Running
profile-central-665dd6977-b258q	Running
queryfacade-central-74bbd477d5-64zkp	Running
refscatalog-central-6996ff7544-lrgkx	Running
structure-central-76d7c74cf6-jkv98	Running
tarantool-central-54b8977f-k84wh	Running
taskscheduler-central-6b9b9fff45-cskq9	Running
tusker-central-c698699bd-b47zk	Running
webgui-central-84fcc4b476-p8jdc	Running

```
*****SUMMARY*****

###docker###
docker was installed 19.3.5

###kubernetes###
kubernetes init scripts apply - done
kubernetes was installed 1.17.1

###Result###
Install product: Infowatch Platform 1.0(platform)
Install node mode: central
Install node label: central
installed 28 components
updated   0 components
web ui:
https://192.158.0.156
```

19. Введите в браузере полученный IP-adress: port (`https://192.158.0.156`), чтобы начать использование Системы.

Подробнее о сервисах Clickhouse, Tarantool, PostgreSQL, Datastorage см. "Глоссарий".

См. также в этом разделе:

- Настройка сетевых правил доступа
- Описание файла лицензии
- Устранение неполадок и восстановление Системы

5.1 Настройка сетевых правил доступа

Для корректной работы InfoWatch Activity Monitor (далее – AM) должны быть разрешены соединения:

Соединение	Порт	Описание
Рабочая станция Администратора → Сервер AM	TCP 22	Используется для управления сервером AM через ssh-консоль
Рабочая станция ОБ → Сервер AM	TCP 443	Используется для доступа Офицера безопасности к Web-консоли AM
Сервер DM → Сервер AM	TCP 17104	Используется для получения данных из InfoWatch Device Monitor
Сервер AM → Веб-сервер Traffic Monitor	TCP 443	Используется для загрузки данных из Traffic Monitor в AM
Сервер AM → LDAP-серверы	TCP 3268 TCP 389	Используются для синхронизации AM с LDAP-каталогами
Сервер AM → LDAPS-серверы	TCP 3269 TCP 636	Используются для синхронизации AM с LDAPS-каталогами
Сервер AM → NTP-серверы	UDP 123	Используется для синхронизации времени
Сервер AM → DNS-серверы	UDP 53	Используется для разрешения DNS-запросов

5.2 Описание файла лицензии

Файл лицензии **am_license_yyyy_mm_dd.license** содержит следующие параметры:

Код	Описание
{	

"Meta": {	
"Version": "1.0",	Версия продукта
"Fingerprint": "40c1ce6...cfed92f",	Цифровой отпечаток
"Signature": "3045022...9923c24"	Цифровая подпись, формируемая на основании цифрового отпечатка
},	
"License": {	Информация о лицензии
"ActiveDays": 30,	Срок действия в днях: • для демонстрационной - по умолчанию 30, максимум 60; • для коммерческой - возможен срочный вариант лицензии со сроком действия N дней или бессрочная лицензия
"Issuer": "InfoWatch",	Эмитент лицензии
"Licensee": "",	Приобретатель лицензии (лицензиат)
"Context": "6d50fdf...a3ec201 fcc0161470 2bb4e0d...0e009fd 616bf57958781d5ee3c02c71b9",	
"Product": "Activity Monitor",	Наименование продукта
"Features": [	
{	
"service": "Dossier",	
"id": "activeUsersCountOnEP",	
"name": "\u041a\u043e\u043b\u0438\u0447\u0435\u0441\u0442\u0432\u043e\u0430\u043a\ u0442\u0438\u0432\u043d\u044b\u0445 \u0434\u043e\u0441\u044c\u0435",	
"type": "int",	Тип данных свойства лицензии

"value": 3	
},	
{	
"service": "Dossier",	
"id": "licenseType",	Тип лицензии: стандартная или корпоративная
"name": "\u0422\u0438\u043f \u043b\u0438\u0446\u0435\u043d\u0437\u0438\u0438",	
"type": "string",	
"value": "trial"	Вид лицензии: демонстрационная или коммерческая
},	
{	
"service": "DataCollector",	
"id": "licenseType",	
"name": "\u0422\u0438\u043f \u043b\u0438\u0446\u0435\u043d\u0437\u0438\u0438",	
"type": "string",	
"value": "trial"	
}] } }	

5.3 Устранение неполадок и восстановление Системы

Во время установки Системы возможны сбои: прерывания работы программы установки, отключение электричества и прочее. В этом случае Система будет установлена некорректно. В качестве решения рекомендуется выполнить сброс Системы, а затем повторить шаги по установке. После сброса все данные сохранятся в Системе, поэтому при повторной установке выберите **нет** в ответ на вопрос об удалении существующих данных.

Чтобы сбросить установку Системы:

1. Перейдите в директорию, где распакован дистрибутив продукта.
2. Выполните команду:
   ```
   ./setup.py reset
   ```

6 Как обновить InfoWatch Activity Monitor

Чтобы обновить Систему:

1. Создайте новую директорию на диске, например, `am_1.0.X`.
   `mkdir am_1.0.X`
2. Скопируйте архив с новой версией `iw_am_setup_1.0.X.XXX.tar.xz` в созданную директорию.
3. Перейдите в эту директорию и распакуйте в ней архив с дистрибутивом продукта:
   `cd am_1.0.X && tar xvf iw_am_setup_1.0.X.XXX.tar.xz`
4. Запустите программу обновления продукта:
   `./setup.py update`
5. Дождитесь окончания процесса обновления. Программа обновит компоненты продукта и установит требуемое окружение.

При успешном обновлении Системы будут:

- обновлены бинарные модули;
- созданы новые схемы БД;
- сохранены все пользовательские настройки, которые были внесены до обновления Системы;
- сохранены все данные, которые были добавлены в Систему.

7 Как удалить InfoWatch Activity Monitor

Чтобы удалить Систему:

1. Перейдите в папку с распакованным продуктом.
2. Выполните команду:
   `./setup.py remove`
3. Дождитесь окончания процесса. Программа удалит компоненты продукта. Данные продукта (события, персоны, рабочие станции, и прочее) будут сохранены. Если необходимо, их можно удалить вручную из папок, указанных при установке.

8 Установка Device Monitor (DM)

Для того, чтобы иметь возможность отправлять события в Систему, необходимо установить сервер DM и настроить параметры соединения с ним. Подробную информацию об установке DM см. в документе "Руководство по установке InfoWatch Traffic Monitor. Установка Системы. Установка InfoWatch Device Monitor".

Примечание:

Отправка событий в Систему возможна для нескольких серверов DM. О том, как настроить отправку, см. в статье "Настройка сервера Device Monitor".