

INFOWATCH

InfoWatch Vision 2.0.0. Руководство по установке

23/05/2020

© 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 Vision 9

5.1 Чтобы установить Систему: 9

5.2 Установка лицензии и плагина в InfoWatch Traffic Monitor 10

5.2.1 Описание архива плагина 11

5.2.2 Описание файла лицензии 12

5.3 Настройка сетевых правил доступа 13

5.4 Устранение неполадок 13

6 Как обновить Vision 14

7 Как удалить Vision 15

В настоящем руководстве вы сможете найти сведения по установке, обновлению и удалению InfoWatch Vision 2.0.0 – программного обеспечения, предназначенного для визуализации расследования инцидентов на основе данных, полученных от InfoWatch Traffic Monitor.

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 Vision 2.0.0 входят:

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

Сопутствующая документация по комплексу InfoWatch Traffic Monitor включает в себя:

- «InfoWatch Traffic Monitor. Руководство по установке». Содержит описание порядка установки, настройки, обновления и удаления системы InfoWatch Traffic Monitor.
- «InfoWatch Traffic Monitor. Руководство администратора». Содержит информацию по администрированию Системы (база данных, серверная часть).
- «InfoWatch Traffic Monitor. Руководство пользователя». Содержит описание порядка работы с InfoWatch Traffic Monitor (настройка конфигурации, экспорт/импорт данных, составление политик для обработки объектов).
- «InfoWatch Traffic Monitor. Справочник по конфигурационным файлам». Содержит пояснения к часто используемым конфигурационным файлам.

3 Техническая поддержка пользователей

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

- если вы приобрели продукт у партнера компании InfoWatch, то обратитесь в службу технической поддержки партнера.
- если продукт приобретен у компании InfoWatch напрямую, то обратитесь в службу технической поддержки компании InfoWatch по адресу support@infowatch.com.

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: https://www.infowatch.ru/support.

Перед обращением в службу технической поддержки рекомендуется посетить раздел База знаний на нашем сайте: https://kb.infowatch.com/. Возможно, там уже содержится ответ на интересующий вас вопрос или описано решение возникшей у вас проблемы.

4 Типы установки, аппаратное и программное обеспечение

Система может иметь 2 варианта установки и размещения относительно сервера Infowatch Traffic Monitor:

- на выделенном сервере для работы с одним или несколькими серверами Traffic Monitor (stand-alone);
- на одном сервере с Traffic Monitor.

Нагрузка на аппаратное обеспечение рассчитывается, исходя из объема анализируемых данных. В таблице приведены минимальные системные требования к объему оперативной памяти и жесткого диска.

<table>
<tr><th rowspan="3">Количество сотрудников</th><th rowspan="3">Количество событий</th><th rowspan="3">Срок хранения событий</th><th colspan="4">Аппаратное обеспечение</th></tr>
<tr><th colspan="2">Установка stand-alone</th><th colspan="2">Установка с Traffic Monitor</th><th rowspan="2">Процессор</th></tr>
<tr><th>RAM</th><th>HDD</th><th>RAM</th><th>HDD</th></tr>
<tr><td>100</td><td>100 тысяч</td><td rowspan="6">3 мес</td><td>4 GB</td><td>330 MB</td><td>16 GB</td><td>50 GB</td><td rowspan="6">Количество ядер - 6,
Частота - 3.1 ГГц,
Разрядность - 64 bit,
Поддержка инструкций SSE 4.2</td></tr>
<tr><td>500</td><td>500 тысяч</td><td>4 GB</td><td>2 GB</td><td>24 GB</td><td>100 GB</td></tr>
<tr><td>1000</td><td>1 миллион</td><td>4 GB</td><td>5 GB</td><td colspan="2" rowspan="4">Совместная установка не рекомендуется по причине высокой нагрузки на аппаратные средства</td></tr>
<tr><td>5 000</td><td>5 миллионов</td><td>8 GB</td><td>20 GB</td></tr>
<tr><td>10 000</td><td>10 миллионов</td><td>16 GB</td><td>35 GB</td></tr>
<tr><td>50 000</td><td>50 миллионов</td><td>32 GB</td><td>160 GB</td></tr>
</table>

Система может быть установлена на ОС:

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

В качестве СУБД используется PostgreSQL.

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

Важно!

Система рекомендована к установке в организациях с Active Directory, где количество пользователей не превышает 100000.

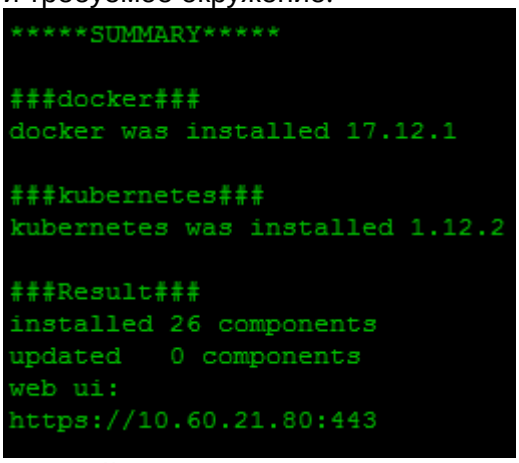
5 Как установить Vision

Дистрибутив продукта представляет собой архив **iw_vision2.0_setup_2.0.0.xxxx.tar.xz,** где xxxx — номер сборки. Этот архив содержит полный набор бинарных модулей образов контейнеров, необходимых для развертывания продукта без доступа к сети Интернет (offline-установка). Кроме этого, данный архив содержит программу установки. Программа установки написана на языке Python версии 2.7, поэтому для установки продукта в целевой ОС установите интерпретатор этого языка.

5.1 Чтобы установить Систему:

1. Создайте целевую директорию на диске - vision:
   `mkdir vision`
2. Скопируйте архив `iw_vision2.0_setup_2.0.0.xxxx.tar.xz` в созданную директорию.
3. Распакуйте архив с дистрибутивом продукта в эту директорию:
   `tar xf ./iw_vision_setup_2.0.xxxx.tar.xz`
   Для установки продукта на ОС CentOS 7 необходим пакет **xz-utils**, устанавливающий инструменты командной строки для работы с форматом сжатия **xz**. Поэтому дополнительно необходимо:
   a. Распаковать архив и получить tar-файл:
      `unxz iw_vision2.0_setup_2.0.0.xxxx.tar.xz`
   b. Распаковать полученный tar-файл в текущую директорию:
      `tar -xvf iw_vision2.0_setup_2.0.0.xxxx.tar`
4. Запустите программу установки продукта:
   `./setup.py install`
5. Ознакомьтесь с условиями лицензионного соглашения. Лицензионное соглашение содержит несколько страниц. Для перехода на следующую страницу используйте клавишу **Enter**.
6. Введите "`y`", чтобы принять лицензионное соглашение, и нажмите **Enter**.
7. Введите IP-адрес рабочей станции формата IPv4: "`xxx.xxx.xxx.xxx`" и нажмите **Enter**.
8. Укажите тип БД (по умолчанию: `iw`) и нажмите **Enter**.
9. Укажите путь для размещения данных Clickhouse (по умолчанию: `/mnt/chdata`) и нажмите **Enter**.
10. Выделите объем дискового пространства в процентах от общего объема диска для `/mnt/chdata` (по умолчанию: 45%) и нажмите **Enter**.
11. Укажите путь для размещения данных Tarantool (по умолчанию: `/mnt/trdata`) и нажмите **Enter**.
12. Выделите объем дискового пространства в процентах от общего объема диска для `/mnt/trdata` (по умолчанию: 45%) и нажмите **Enter**.
13. Укажите путь для размещения данных PostgreSQL (по умолчанию: `/mnt/pgdata`) и нажмите **Enter**.
14. Выделите объем дискового пространства в процентах от общего объема диска для `/mnt/pgdata` (по умолчанию: 10%) и нажмите **Enter**.
15. Укажите порт подключения к веб-интерфейсу (по умолчанию: `443`) и нажмите **Enter**.

16. Дождитесь окончания процесса установки. Программа установит компоненты продукта и требуемое окружение.



17. Настройте правила POD сети (подробнее см. "Конфликты при взаимодействии службы firewalld и Kubernetes", "Полное отключение межсетевого экрана").
18. Введите полученный IP-adress:port (`https://10.60.21.80:443`) в своем браузере, чтобы начать использование Системы.

В этом разделе:

- Установка лицензии и плагина в InfoWatch Traffic Monitor
- Настройка сетевых правил доступа
- Устранение неполадок

5.2 Установка лицензии и плагина в InfoWatch Traffic Monitor

Чтобы установить лицензию:

1. Войдите под учетной записью Офицера безопасности в Консоль управления сервера Traffic Monitor, данные которого требуется синхронизировать.
2. Перейдите в раздел **Управление** -> **Лицензии.**
3. В области **Лицензии** нажмите **+**.
4. В открывшемся окне нажмите **Загрузить**.
5. Добавьте полученный от сотрудников Технической поддержки InfoWatch файл лицензии **tm_license_yyyy_mm_dd.license**, используя Проводник. После успешного добавления лицензии информация о ней будет доступна в разделе **Управление** -> **Лицензии.**

> **Важно!**
>
> В лицензии для Traffic Monitor должны быть указаны компания, выпускающая лицензию (**IW**) и система-получатель данных (**Vision**).

Для установки соединения и последующего получения данных из Traffic Monitor необходимо установить плагин InfoWatch Vision в Консоли управления Traffic Monitor. Расположение zip-архива с файлом: `iw_vision2.0_setup_2.0.0.x.tar/tmplugin/vision.zip`

Чтобы установить плагин:

1. Войдите под учетной записью Офицера безопасности в Консоль управления сервера Traffic Monitor, данные которого требуется синхронизировать.

2. Перейдите в раздел **Управление** -> **Плагины**.



3. В области **Плагины** нажмите.
4. В открывшемся окне нажмите **Загрузить**.
5. Добавьте архив с файлом плагина, используя Проводник.

После успешного добавления плагина информация о нем будет доступна в разделе **Управление** -> **Плагины.** Для последующего получения данных из Traffic Monitor необходим токен, который создается автоматически и доступен в разделе **Управление** -> **Плагины** -> **Токены.** Скопируйте выданный токен и укажите его в поле **Токен** в консоли InfoWatch Vision при настройке интеграции.

Описание файла лицензии и архива плагина см. в "Описание файла лицензии" и "Описание архива плагина". В статье "Как привязать плагин к лицензии" описано, как загрузить плагин и лицензию в Traffic Monitor одним архивом.

5.2.1 Описание архива плагина

Плагин представляет собой архив в формате **.zip**. В состав архива входит файл **manifest.json**, содержащий информацию о плагине:

Код	Описание
`{`	
`"PLUGIN_ID": "2C1D7336267741DF9FC226297503CAFF",`	Уникальный 128-битный идентификатор (UUID) плагина
`"DISPLAY_NAME": "InfoWatch Vision",`	Уникальное название плагина
`"DESCRIPTION": "InfoWatch Vision",`	Описание плагина
`"VERSION": "2.0.0",`	Версия плагина
`"IS_SYSTEM": false,`	Признак "Предустановленный", который означает, установлен ли данный плагин по умолчанию
`"VENDOR": "IW",`	Идентификатор компании-разработчика, который соответствует названию компании в лицензии
`"PATTERN_SEARCH_LICENSE": "{\"operator\":\"or\",\"conditions\": [{\"importer_name\":\"Vision\"}]}",`	Шаблон для поиска ранее загруженных лицензий для привязки их к плагину
`"DATA_RECEIVER": ["Vision"],`	Система-получатель событий

`"LICENSE": [ ]`	Секция путей к файлам лицензий
	Пример:
	`"LICENSE": [`
	`{"PATH":"licenses/файл лицензии 1.license"},`
	`{"PATH":"licenses/файл лицензии 2.license"},`
	`],`

}	

5.2.2 Описание файла лицензии

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

Код	Описание
{	
"License": {	Описание лицензии
"ActiveDays": 60,	Срок действия в днях: • для демонстрационной - по умолчанию 30, максимум 60; • для коммерческой - 365
"Features": [	Лицензируемые каналы
{	
"common_name": "IW",	Компания, выпускающая лицензию
"importer_name": "Vision"	Система-получатель данных ТМ
}	
],	
"Signature": "304502206a59cc72611dffe2a4a73e4e08e2b5386edf8d8fc336fd2f40ae643e",	Цифровая подпись, формируемая на основании цифрового отпечатка
"Licensee": "",	Приобретатель лицензии (лицензиат)
"Meta": {	Параметры лицензии
"restrictions": "demo",	Вид лицензии: демонстрационная или коммерческая
"type": "standard",	Тип лицензии: стандартная или корпоративная
"users": "10000",	Максимально допустимое количество пользователей
"context": "3eeaa674ef003f48762287379980888ce1a9b6dc5b65435be66dd3eb258e7b5afb"	
},	

"Fingerprint": "002704ff708441611350b7f0368ef082201f7e509f953b618db63fcb4e9abbe7",	Цифровой отпечаток
"IssueDate": "2019-08-06",	Дата начала действия
"Issuer": "InfoWatch"	Эмитент лицензии
}	
}	

5.3 Настройка сетевых правил доступа

Для корректной работы Системы должны быть разрешены следующие соединения:

Соединение	Порт	Описание
Рабочая станция Администратора → Сервер Vision 2.0	TCP 22	Используется для управления сервером Vision 2.0 через ssh-консоль
Рабочая станция ОБ → Сервер Vision 2.0	TCP 443	Используется для доступа Офицера безопасности к Web-консоли Vision 2.0
Сервер Vision 2.0 → Веб-сервер Traffic Monitor	TCP 443	Используется для загрузки данных из Traffic Monitor в Vision 2.0
Сервер Vision 2.0 → LDAP-серверы	TCP 3268 TCP 389	Используются для синхронизации Vision 2.0 с LDAP-каталогами
Сервер Vision 2.0 → NTP-серверы	UDP 123	Используется для синхронизации времени
Сервер Vision 2.0 → DNS-серверы	UDP 53	Используется для разрешения DNS-запросов

5.4 Устранение неполадок

Во время установки Системы возможны сбои: прерывания работы программы установки, отключение электричества и т.д. В этом случае Система будет установлена некорректно. Для решения этой проблемы следует запустить функционал сброса. После сброса все шаги по установке необходимо повторить.

Чтобы сбросить установку Системы:

1. Перейдите в директорию, где установлена Система.
2. Выполните команду:
   ```
   ./setup.py reset
   ```

6 Как обновить Vision

> **Важно!**
>
> Обновление с Vision 1.0 на текущую версию не поддерживается. Необходимо пройти процесс полной установки Системы (см. "Как установить Vision").

Чтобы обновить Систему:

1. Скопируйте архив с новой версией **iw_vision2.0_setup_2.0.0.xxxx.tar.xz** в директорию установки.
2. Распакуйте архив с дистрибутивом продукта в эту директорию:
   `tar -xfJ ./iw_vision2.0_setup_2.0.0.xxxx.tar.xz`
3. Запустите программу обновления продукта:
   `./setup.py update`

При обновлении Системы будут сохранены все пользовательские настройки, которые были внесены до обновления Системы, и все данные, которые были добавлены в Систему.

7 Как удалить Vision

Чтобы удалить Систему:

1. Перейдите в папку с последней версией продукта.
2. Выполните команду:
   `./setup.py remove`
3. Дождитесь окончания процесса. Программа удалит компоненты продукта. Данные продукта удалены не будут. Если необходимо, их можно удалить вручную из папок, указанных при установке.