



INFOWATCH

InfoWatch Data Discovery. Руководство по
установке, конфигурированию и
администрированию

10/03/2022

© АО "ИнфоВотч"

Тел./Факс +7 (495) 229-00-22

<http://www.infowatch.ru>

СОДЕРЖАНИЕ

1	Обзор	4
1.1	Функциональные возможности Data Discovery	4
2	Аппаратные и программные требования	5
2.1	Аппаратные требования.....	5
2.2	Программные требования.....	5
3	Установка Data Discovery	7
3.1	Чтобы установить Систему:.....	7
4	Установка лицензии и плагина Traffic Monitor	10
5	Настройка сетевых правил доступа	11
6	Устранение неполадок	12
7	Удаление Data Discovery	13
8	Настройки пользователей	14
8.1	Пользователи	14
8.1.1	Создание нового пользователя	14
8.1.2	Редактирование учетной записи	15
8.1.3	Просмотр профиля пользователя.....	16
8.1.4	Смена пароля пользователя	17
8.1.5	Активация и деактивация пользователя	17
8.1.6	Удаление пользователя.....	17
8.2	Роли	18
8.2.1	Создание и настройка роли.....	18
8.2.2	Просмотр и редактирование роли	19
8.2.3	Снятие и удаление роли пользователя	20
9	Настройки Системы	22
9.1	Управление безопасностью.....	22
9.2	Мониторинг состояния Системы	23
10	Настройки продукта	26

В настоящем руководстве содержится описание InfoWatch Data Discovery, а также инструкция по установке, настройке и запуску данной Системы.

Аудитория

Данное руководство предназначено для инженеров внедрения и офицеров безопасности, которые имеют соответствующую квалификацию и полномочия для работы с Системой и ее администрирования.

Руководство рассчитано на пользователей, знакомых с основами работы в среде операционных систем Linux и СУБД PostgreSQL.

Комплект документов

В комплект документации входят:

- «InfoWatch Data Discovery. Руководство по установке, конфигурированию и администрированию». Документ содержит описание процесса установки Системы, ее настройки, а также удаления.
- «InfoWatch Data Discovery. Руководство пользователя». Содержит описание порядка работ для решения задач сканирования.

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 InfoWatch Traffic Monitor (база данных, серверная часть).
- «InfoWatch Traffic Monitor. Руководство пользователя». Содержит описание порядка работы с InfoWatch Traffic Monitor (настройка конфигурации, экспорт/импорт данных, подготовка политик для обработки объектов).
- «InfoWatch Traffic Monitor. Справочник по конфигурационным файлам». Содержит пояснения к часто используемым конфигурационным файлам.

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 РФ. Вы также можете посетить раздел технической поддержки на нашем сайте: <https://www.infowatch.ru/services/support>.

1 Обзор

Система InfoWatch Data Discovery (далее Data Discovery) предназначена для реализации созданных в InfoWatch Traffic Monitor (далее Traffic Monitor) политик защиты данных на компьютерах и серверах. Система позволяет подключаться по протоколам SMB и SSH к файловым хранилищам удаленных компьютеров и к рабочим станциям под управлением Linux, сканировать файлы и отправлять их копии на сервер Traffic Monitor для анализа и формирования событий в соответствии с настроенными политиками безопасности.

1.1 Функциональные возможности Data Discovery

- сканирование общих сетевых ресурсов по протоколу SMB;
- сканирование рабочих станций под управлением Linux по протоколу SSH;
- создание копий файлов;
- отправка файлов на сервер Traffic Monitor;
- обнаружение и обработка новых и измененных файлов на ресурсах с последующей их отправкой в Traffic Monitor;
- подготовка и отображение статистики выполнения задач сканирования.

2 Аппаратные и программные требования

2.1 Аппаратные требования

Аппаратные требования и число необходимых серверов Data Discovery зависят от сетевого окружения и предполагаемой нагрузки. Ниже приведена примерная конфигурация для обработки 50 хостов в одной задаче сканирования:

ЦПУ	8 ядер, 16 потоков Intel Xeon или аналог
ОЗУ	24 GB
Диск	raid5 10k HDD
Сеть	1 Gbps LAN

2.2 Программные требования

Для установки и работы Системы может быть использовано следующее программное обеспечение:

Тип ПО	Варианты
Операционная система	<ul style="list-style-type: none">• Astra Linux Special Edition 1.6 "Смоленск" (все обновления безопасности);• Red Hat Enterprise Linux 7.5 и более поздние;• Oracle Linux 7.0 и более поздние.
СУБД	PostgreSQL 12
Браузер	<ul style="list-style-type: none">• Google Chrome;• Яндекс.Браузер. <div style="border: 1px solid red; padding: 5px; margin-top: 10px;"><p>⚠ Важно!</p><p>В браузере должна быть реализована аппаратная поддержка WebGL/WebGL2</p></div>

⚠ Важно!

Data Discovery взаимодействует с InfoWatch Traffic Monitor 6.10.15 и выше, но в рамках версии 6.10, а также с версиями 7.1.X, 7.2.X и 7.3.0.

 **Важно!**

Data Discovery должен быть установлен на отдельный сервер. Не рекомендуется совместная установка с другими продуктами.

3 Установка Data Discovery

Дистрибутив продукта представляет собой архив `iw_discovery_setup_x.x.x.xxx.tar.xz`, где `x.x.x.xxx` – номер версии. 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.

Установка Data Discovery производится вручную, при помощи командной строки.

⚠ Важно!

Data Discovery должен быть установлен на отдельный сервер. Не рекомендуется совместная установка с другими продуктами.

⚠ Важно!

Для корректной работы используемого Системой Docker 19.03 в окружении 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. статьи Базы знаний "Конфликты при взаимодействии службы `firewalld` и `Kubernetes`", "Полное отключение межсетевого экрана"). В противном случае установка продукта будет невозможна.

3.1 Чтобы установить Систему:

1. Создайте новую директорию на диске (например, `discovery`):
`mkdir discovery`
2. Скопируйте архив `iw_discovery_setup_x.x.x.xxx.tar.xz` в созданную директорию.
3. Распакуйте архив с дистрибутивом продукта в эту директорию:
`tar xf iw_discovery_setup_x.x.x.xxx.tar.xz`
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 сетевого интерфейса для взаимодействия с кластером в формате IPv4: "xxx.xxx.xxx.xxx" (по умолчанию: 0.0.0.0) и нажмите **Enter**.

Примечание:

Здесь и далее для использования параметров, предложенных по умолчанию, нажмите **Enter** без ввода значений.

8. Выделите объем оперативной памяти для размещения данных Clickhouse (по умолчанию: 80%) и нажмите **Enter**.
9. Укажите путь для размещения данных Clickhouse (по умолчанию: /mnt/chdata) и нажмите **Enter**.
10. Укажите путь для размещения данных Tarantool (по умолчанию: /mnt/trdata) и нажмите **Enter**.
11. Укажите путь для размещения данных PostgreSQL (по умолчанию: /mnt/pgdata) и нажмите **Enter**.
12. Укажите путь для размещения бинарных данных (по умолчанию: /mnt/dsdata) и нажмите **Enter**.
13. Укажите порт подключения к веб-интерфейсу (по умолчанию: 443) и нажмите **Enter**.
14. Дождитесь окончания процесса установки продуктовой платформы.
15. Ознакомьтесь с отчетом об установке платформы (в нашем примере была установлена платформа версии 1.4.0.162). В графе **web ui** указаны адрес и порт для подключения к веб-интерфейсу (в нашем примере – <https://10.60.21.130:443>):

```
###Result###
Install product: Infowatch Platform(platform) Version: 1.4.0.162
Install node mode: central
Install node label: central
installed 32 components
updated 0 components
add ref 0 components
web ui:
https://10.60.21.130:443
```

16. Укажите путь для временного размещения копий сканированных файлов (по умолчанию: /mnt/disctps) и нажмите **Enter**.
17. Дождитесь окончания процесса установки продукта Data Discovery.
18. Ознакомьтесь с отчетом об установке продукта (в нашем примере был установлен Data Discovery версии 1.1.0.30):

```
###Result###
Install product: Infowatch Data Discovery(discovery) Version: 1.1.0.30
Install node mode: central
Install node label: central
installed 1 components
updated 0 components
add ref 0 components
```

19. Убедитесь что все сервисы запущены, выполнив команду:
`kubectl get pods -n infowatch`


NAME	READY	STATUS	RESTARTS	AGE
clickhouse-central-66b6757967-xw59f	1/1	Running	0	27m
cluster-agent-6gg7b	1/1	Running	0	27m
cluster-central-f7c5d6969-s9ks9	1/1	Running	0	27m
comment-central-74cb6888d4-74fwv	1/1	Running	0	27m
configstorage-central-cbf85c4f8-wdhsK	1/1	Running	0	12m
datastorage-central-5c97b867f7-lskzj	1/1	Running	0	27m
department-central-546486967c-nxlvz	1/1	Running	0	27m
dicsyncdrvldap-central-7598c7d497-g9pmn	1/1	Running	0	27m
dicsyncdrvtm-central-949d89bd9-h9xxd	1/1	Running	0	27m
dictionary-central-5dff67f7c6-brbp8	1/1	Running	0	27m
discoveroperator-central-6cfcbb8647-8hkzv	1/1	Running	0	12m
dossier-central-56b76b86bb-xw4rp	1/1	Running	0	27m
epevents-central-86dd56fbb-dqzrn	1/1	Running	0	27m
factsstorage-central-5f59fb59f9-s5wdv	1/1	Running	0	27m
guard-central-879c574b6-vf7jp	1/1	Running	0	12m
guiapps-central-98fb6b56f-rgmcc	1/1	Running	0	12m
intcoordinator-central-7fbf554b75-bg7cx	1/1	Running	0	27m
license-central-8544ff968d-hzhsp	1/1	Running	0	27m
nats-central-8c7ccb957-j87jg	1/1	Running	0	27m
pobjects-central-f75b847d-wkhgv	1/1	Running	0	27m
policy-central-65bc6895f4-qr6gs	1/1	Running	0	27m
postgres-central-8b96d97dc-k2dd8	1/1	Running	0	27m
profile-central-58669fc78f-hgjcg	1/1	Running	0	27m
queryfacade-central-5bc5f7fbf-m7t2z	1/1	Running	0	27m
refscatalog-central-6fbfdf889f-mxdx5	1/1	Running	0	27m
report-central-554564df9-4rgnf	1/1	Running	0	27m
structure-central-6cb9cf68c8-9nlhw	1/1	Running	0	27m
tarantool-central-5c889c47d5-2htcg	1/1	Running	0	27m
taskscheduler-central-65db98b84b-z499v	1/1	Running	0	27m
tusker-central-7c7fd7b58b-k5dnf	1/1	Running	0	27m
webgui-central-7f6765f6f8-wp8th	1/1	Running	0	12m

20. Введите адрес и порт для подключения к веб-интерфейсу (в нашем примере – <https://10.60.21.130:443>) в браузере, чтобы начать использование Системы (см. Шаг 15 данной инструкции).

4 Установка лицензии и плагина Traffic Monitor

Для установки соединения и последующей отправки данных в Traffic Monitor необходимо установить лицензию и плагин в Консоли управления 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 Лицензии нажмите .
4. В открывшемся окне нажмите **Загрузить**.
5. Добавьте полученный от сотрудников Технической поддержки InfoWatch файл лицензии вида **tm_license_yyyy_mm_dd.license**, используя Проводник. После успешного добавления лицензии информация о ней будет доступна в разделе **Управление -> Лицензии**.

Для экспорта данных в Консоли управления Traffic Monitor используйте предустановленный плагин InfoWatch Crawler. Плагин будет отображаться только если в Системе установлена действующая лицензия (см. "InfoWatch Traffic Monitor. Руководство пользователя", раздел "Управление лицензиями").

Информация о плагине будет доступна в разделе **Управление -> Плагины**. Для последующей отправки данных в Traffic Monitor необходим токен, который создается автоматически и доступен в разделе **Управление -> Плагины -> Токены**. Скопируйте выданный вам токен и укажите его в поле **Токен** в Консоли управления Data Discovery при настройке экспорта данных. Подробнее см. "InfoWatch Data Discovery. Руководство пользователя", "Настройка интеграции с Traffic Monitor".

5 Настройка сетевых правил доступа

Для корректной работы Data Discovery должны быть разрешены соединения:

Соединение	Порт	Описание
Рабочая станция Офицера Безопасности → Сервер Data Discovery	TCP 443	Используется для доступа Офицера безопасности к Web-консоли Data Discovery
Сервер Data Discovery → Веб-сервер Traffic Monitor	TCP 443	Используется для загрузки данных из Data Discovery в Traffic Monitor
Сервер Data Discovery → NTP-серверы	UDP 123	Используется для синхронизации времени

6 Устранение неполадок

Во время установки Системы возможны сбои: прерывания работы программы установки, отключение электричества и т.д. В таком случае Система будет установлена некорректно. В случае возникновения подобной ситуации следует запустить функционал сброса. После сброса все шаги по установке необходимо повторить. После сброса все данные сохраняются в Системе. Поэтому при повторной установке на вопрос об удалении существующих данных выберите ответ **Нет**.

Чтобы сбросить установку Системы:


1. Перейдите в директорию, куда должна была быть установлена Система.
2. Выполните команду:
`./setup.py reset`

7 Удаление Data Discovery

Чтобы удалить Систему:

1. Перейдите в папку с версией продукта.
2. Выполните команду:
`./setup.py remove`
3. Дождитесь окончания процесса. Программа удалит компоненты продукта. Данные продукта удалены не будут. При необходимости вы можете удалить данные вручную из папок, указанных при установке.

8 Настройки пользователей

Переход к настройкам осуществляется при нажатии  в правой верхней части экрана. В разделе содержится информация по настройке пользователей Системы и их ролей:

- [Пользователи](#)
- [Роли](#)

8.1 Пользователи

Во время установки Системы создается предустановленный пользователь – Главный офицер. Для входа в Систему введите логин и пароль по умолчанию:

Логин	Пароль
officer	xxXX1234

При первом входе в Систему Офицеру безопасности необходимо сменить пароль на постоянный (см. "Смена пароля пользователя").

Главная страница раздела **Пользователи** содержит список пользователей, допущенных к работе с Системой:

- Главного Офицера безопасности;
- других Офицеров безопасности (ОБ), подчиненных ему.

Целевые действия:

- [Создание нового пользователя](#)
- [Редактирование учетной записи](#)
- [Просмотр профиля пользователя](#)
- [Смена пароля пользователя](#)
- [Активация и деактивация пользователя](#)
- [Удаление пользователя](#)

8.1.1 Создание нового пользователя

Главный офицер может добавить новых пользователей, которые также могут выполнять функции Офицеров безопасности. Для этого:

1. Перейдите в раздел **Настройки -> Пользователи**.
2. Нажмите **+ Создать**.
3. Введите параметры согласно таблице:



Параметр	Обязательный параметр	Описание
<i>Фотография</i>	Нет	Фотография пользователя
<i>Имя пользователя</i>	Да	Имя нового пользователя (правила см. Управление безопасностью).

Параметр	Обязательный параметр	Описание
<i>Логин</i>	Да	Имя учетной записи пользователя (правила см. Управление безопасностью). Логин не зависит от верхнего или нижнего регистра
<i>Пароль</i>	Да	Пароль учетной записи (правила см. Управление безопасностью)
<i>Подтверждение пароля</i>	Да	Пароль учетной записи
<i>Роли</i>	Нет	Роль пользователя в Системе. Пользователю может быть присвоена только одна роль.
<i>Язык консоли</i>	Нет	Язык интерфейса для нового пользователя: <i>Русский</i> или <i>Английский</i>
<i>Контакты</i>	Нет	Номер мобильного телефона или email-адрес. Можно добавить одно или несколько значений



4. Нажмите **Создать**. Новый пользователь будет добавлен в Систему. При первом входе в Систему он должен поменять пароль своей учетной записи (см. "[Смена пароля пользователя](#)").

8.1.2 Редактирование учетной записи

Для внесения изменений в учетную запись пользователя:

1. Перейдите в раздел **Настройки** -> **Пользователи**.
2. Нажмите  напротив пользователя (или  на странице профиля пользователя).
3. Выберите **Редактировать**.
4. В открывшемся окне измените одну или несколько настроек. Доступны настройки, заданные при создании пользователя (см. "[Создание нового пользователя](#)").
5. Нажмите **Сохранить**. Новые настройки вступят в силу.

Чтобы назначить роль пользователю:

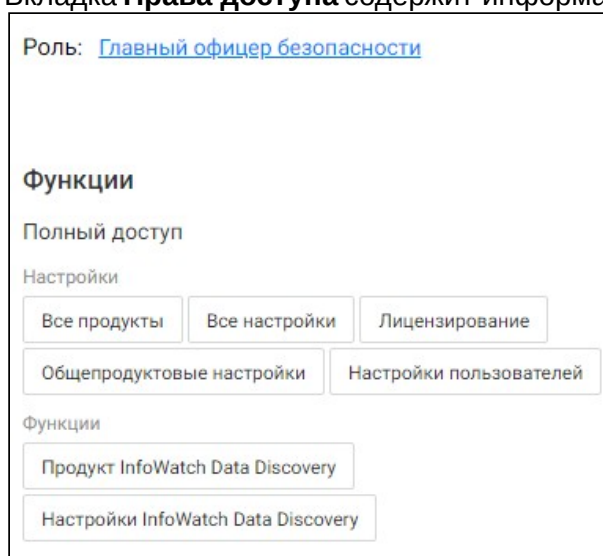
1. Перейдите в раздел **Настройки**  -> **Настройки пользователей** -> **Пользователи**.
2. Кликом выберите пользователя, затем нажмите  в его личной карточке.
3. В личной карточке пользователя перейдите на вкладку **Права доступа** и нажмите на ссылку [Назначить роль](#).
4. В открывшемся окне в поле **Роли** выберите роль для назначения пользователю в раскрывающемся списке. Пользователь без роли не сможет работать в Системе.
5. Нажмите **Сохранить**.

- Чтобы применить изменения, пользователь с данной ролью должен выйти из Системы и пройти повторную авторизацию. Для принудительного завершения сессии данного пользователя, в открывшемся диалоговом окне отметьте **Завершить активные сессии пользователей**.
- Подтвердите действие, нажав **Применить**. Пользователю будет назначена новая роль.

8.1.3 Просмотр профиля пользователя

На странице профиля представлены:

- Вкладка **Персональная информация** содержит данные, указанные при создании:
 - фото пользователя;
 - имя пользователя;
 - логин пользователя в Системе;
 - язык, используемый пользователем в Системе;
 - статус пользователя: ● - активный, ● - деактивирован;
 - контактные данные: номера телефонов, адреса электронной почты;
 - журнал последних активностей с учетной записью ⓘ.
- Вкладка **Права доступа** содержит информацию о правах пользователя в Системе:



- роль, назначенная пользователю;
- доступные для выполнения функции:
 - доступ, который имеет данный пользователь к настройкам и продуктам;
 - объем данных, к которым пользователь имеет доступ.



Удаление или назначение новой роли осуществляется в окне редактирования учетной записи (см. "Редактирование учетной записи").

Действия пользователя:

- [Редактирование учетной записи](#)
- [Смена пароля пользователя](#)
- [Активация и деактивация пользователя](#)

8.1.4 Смена пароля пользователя

Чтобы сменить выданный пароль при первом входе в Систему или скомпрометированный пароль:



1. Нажмите  напротив пользователя (для которого необходимо внести изменение) в разделе **Настройки -> Пользователи** или  в профиле пользователя.
2. Выберите **Смена пароля**.
3. Заполните поля:

Поле	Описание
<i>Старый пароль</i>	Введите действующий пароль
<i>Новый пароль</i>	Введите новый пароль. Новый пароль должен удовлетворять настройкам безопасности (см. " Управление безопасностью ")
<i>Подтверждение пароля</i>	Введите повторно новый пароль



4. Нажмите **Сохранить**.

8.1.5 Активация и деактивация пользователя

Главный офицер может запретить выбранному пользователю выполнять любые действия в Системе. Для этого:



1. Перейдите в раздел **Настройки -> Пользователи**.
2. Напротив требуемого пользователя нажмите  (или  в профиле пользователя),
3. Выберите **Деактивировать**. Учетная запись пользователя будет заблокирована.

Чтобы разблокировать ранее заблокированную учетную запись:

1. Перейдите в раздел **Настройки -> Пользователи**.
2. Напротив заблокированного пользователя нажмите  (или  в профиле пользователя),
3. Выберите **Активировать**. Разблокированный пользователь может снова работать в Системе.

8.1.6 Удаление пользователя


Главный офицер может удалять учетные записи пользователей. Для этого:

1. Перейдите в раздел **Настройки -> Пользователи**.
2. Нажмите  напротив пользователя (или  на странице профиля пользователя).
3. Выберите **Удалить**.
4. В открывшемся окне нажмите **ОК**. Учетная запись пользователя со всеми данными будет удалена без возможности восстановления.

Учетная запись Главного офицера удалению не подлежит.

8.2 Роли

Пользователи Системы могут иметь разные роли, которые определяют их права в Системе. Один пользователь может иметь только одну роль. В случае, если пользователю не назначена ни одна роль, его доступ в Систему невозможен.

На главной странице раздела **Настройки**  -> **Настройки пользователей** -> **Роли** отображены все используемые в Системе роли. Они включают в себя вновь созданные пользовательские роли и две предустановленные:

1. **Главный офицер** – имеет полный доступ ко всем данным Системы, ее настройкам и управлению ролями, включая:
 - создание новых пользователей;
 - создание новых ролей и назначение их пользователям.
2. **Офицер безопасности** – имеет полный доступ к данным Системы, за исключением раздела **Настройки**.



Целевые действия:

- [Создание и настройка роли](#)
- [Просмотр и редактирование роли](#)
- [Снятие и удаление роли](#)

8.2.1 Создание и настройка роли

Пользователь Системы с ролью *Главный офицер безопасности* может создавать новые роли и назначать их пользователям, которые будут выполнять различные функции и работать с данными в рамках назначенной роли. Если у всех пользователей разные компетенции, то необходимо создать столько ролей, сколько пользователей, и в этих ролях указать все необходимые условия. В случае изменения компетенций, необходимо либо скорректировать роль, либо создать новую роль, которую затем следует назначить вместо старой.

Чтобы создать роль:

1. Перейдите в раздел **Настройки**  -> **Настройки пользователей** -> **Роли**.
2. Нажмите **+ Создать**.
3. В открывшемся окне введите название роли и, если необходимо, краткое описание.
4. Нажмите **Сохранить**.
5. На вкладке **Функции** определите доступ пользователя с данной ролью к продукту Data Discovery (по умолчанию доступ запрещен). При выборе будет предоставлен полный доступ. Если доступа не предоставлено, пользователь не сможет авторизоваться в продукте. Отметьте в списке настроек:
 - i. , если необходим полный доступ (просмотр и редактирование) пользователя к настройкам в разделе  . По умолчанию доступ запрещен;
 - ii. , если необходимы права только на просмотр выбранных разделов;
 - iii. , если необходимо запретить доступ к отдельным разделам.
6. По умолчанию запрещен доступ ко всем данным. На вкладке **Данные** можно настроить, как разрешить или ограничить доступ к данным пользователю. Для изменения прав доступа пользователю к выборочным данным, укажите их в категориях: *Персоны, Группы, Филиалы, Контакты, Отделы*. При этом возможно:
 - a. - ограничить доступ к выбранным данным;

- b. - разрешить доступ к выбранным данным;
- c. - закрыть доступ к выбранным данным.

Пример:

Если отметить *Персону* знаком , то эта роль запретит пользователю доступ к любой информации о ней в Системе.

Если отметить *Персону* знаком (или оставить по умолчанию у всех *Персон*), то эта роль предоставит пользователю полный доступ к данным персоны.

Если отметить *Персону* знаком при одновременном выборе других *Персон*, то эта роль предоставит пользователю доступ к информации с участием разрешенных участников ().

Примечание:

Главному офицеру безопасности необходимо внимательно следить за добавляемыми условиями, так как в случае использования различных элементов в роли может получиться не расширение, а сужение доступных данных из-за использования между разными категориями оператора И.


Например: был настроен доступ к Группе-1 ИЛИ Группе-2. Затем добавили доступ к Персоне-1, Персоне-2, Персоне-3. В итоге количество доступных пользователю данных уменьшилось, потому что получилось условие: (Группа-1 ИЛИ Группа-2) И (Персона-1 ИЛИ Персона-2 ИЛИ Персона-3).




Чтобы настроить общее ограничение и на группы и на персоны, Офицер безопасности должен создать в Traffic Monitor сводную группу, которая бы включала в себя все необходимые группы и персоны, и использовать в настройках доступа сводную группу.

- 7. Если требуется закрыть доступ ко всем данным, отметьте **Запретить доступ к данным.**
- 8. На вкладке **Пользователи** выберите доступного пользователя без роли, которому необходимо назначить данную роль. Для этого:
 - a. Нажмите **+ Добавить**;
 - b. В открывшемся диалоговом окне выберите пользователя в поле **Пользователи**;
 - c. Нажмите **Выдать**. Роль будет назначена данному пользователю.
- 9. После внесения всех настроек нажмите **Применить**.
- 10. Для применения настроек, пользователи должны выйти из системы и повторно авторизоваться. Чтобы принудительно завершить сессии пользователей с данной ролью, отметьте **Завершить активные сессии пользователей** в открывшемся окне, а затем нажмите **Применить**.

8.2.2 Просмотр и редактирование роли

Главный офицер может просматривать и редактировать выданные пользователям роли в их личных профилях. Для этого:


- 1. Перейдите в раздел **Настройки**  -> **Настройки пользователей** -> **Пользователи**.
- 2. Кликком выберите пользователя, профиль которого необходимо просмотреть. На странице профиля представлена карточка пользователя с его личными данными.
- 3. Перейдите на вкладку **Права доступа**. На вкладке содержится информация о назначенной пользователю роли, а также:
 - функции – имеет ли пользователь доступ к настройкам продукта;

- данные (области видимости) – объем данных, к которым пользователь имеет доступ.
4. Чтобы поменять роль пользователю, нажмите  и выберите **Редактировать**.
 5. В открывшемся окне сначала удалите настоящую роль, нажав .
 6. Назначьте новую роль, нажав  и кликом выбрав необходимую роль из списка.
 7. Нажмите **Сохранить**, чтобы применить изменения.
 8. Для применения настроек, пользователь должен выйти из Системы и повторно авторизоваться. Чтобы принудительно завершить сессию пользователей с данной ролью, отметьте **Завершить активные сессии пользователей** в открывшемся окне, а затем нажмите **Применить**.





8.2.3 Снятие и удаление роли пользователя

Пользователь не может иметь несколько ролей одновременно. Поэтому если требуется выдать пользователю новую роль, нужно снять действующую.

Чтобы снять роль в карточке роли:




1. Перейдите в раздел **Настройки**  -> **Настройки пользователей** -> **Роли**.
2. Кликком выберите роль, которую необходимо удалить для определенного пользователя (пользователей).
3. Перейдите на вкладку **Пользователи**.
4. Отметьте пользователей, у которых необходимо снять данную роль.
5. Нажмите **Удалить**. Для данных пользователей роль будет снята. После этого можно назначить ему/им другую роль.

Чтобы снять роль в карточке пользователя:

1. Перейдите в раздел **Настройки**  -> **Настройки пользователей** -> **Пользователи**.
2. Далее на выбор:
 - a. нажмите  на плашке пользователя, для которого необходимо удалить данную роль.
 - b. или кликом выберите пользователя, затем нажмите  в его личной карточке.
3. В меню выберите **Редактировать**.
4. В открывшемся окне в поле **Роли** удалите роль пользователя, нажав .
5. Нажмите **Сохранить**.
6. Чтобы применить изменения, пользователь с данной ролью должен выйти из Системы и пройти повторную авторизацию. Для принудительного завершения сессии данного пользователя, в открывшемся диалоговом окне отметьте **Завершить активные сессии пользователей**.
7. Подтвердите действие, нажав **Применить**. У данного пользователя роль будет снята.


Главный офицер может удалять любые роли, кроме предустановленных.

Чтобы удалить роль из Системы:

1. Перейдите в раздел **Настройки**  -> **Настройки пользователей** -> **Роли**.
2. Далее на выбор:
 - a. Нажмите  на плашке пользовательской роли, которую требуется удалить
 - b. или кликом выберите роль, затем нажмите .

3. В окне меню выберите **Удалить**.
4. Чтобы применить изменения, пользователи с данной ролью должны выйти из Системы и пройти повторную авторизацию. Для принудительного завершения сессий данных пользователей, в открывшемся диалоговом окне отметьте **Завершить активные сессии пользователей**.
5. Подтвердите действие, нажав **Удалить**. Если роль была назначена пользователям, она будет снята для них и удалена из списка ролей.

9 Настройки Системы

Переход к настройкам осуществляется при нажатии  в правой верхней части экрана. В разделе содержится информация по следующим настройкам Системы:

- [Настройки пароля](#)
- [Состояние системы](#)

Важно!

Подразделы **Основные настройки** и **Лицензирование** не относятся к продукту Data Discovery в текущей реализации.

9.1 Управление безопасностью

Чтобы предотвратить несанкционированный вход в Систему и максимально обезопасить пользователя от компрометации его учетных данных третьими лицами, Офицер безопасности может устанавливать правила формирования паролей учетных записей и их сроки действия. Для этого:

1. Перейдите в раздел **Настройки** -> **Настройки пароля**.
2. В открывшемся окне установлены настройки по умолчанию. Чтобы ввести новые требования к паролю учетной записи, измените параметры:

Параметр	Описание
<i>Буквы</i>	Заглавные и строчные буквы русского и латинского алфавитов, которые используются для составления пароля. Можно установить: - обязательно для ввода (<input checked="" type="checkbox"/>) – обязательно присутствие букв в пароле - опционально (<input type="checkbox"/>) – допускается пароль без букв
<i>Цифры</i>	Арабские цифры, которые используются для составления пароля. Можно установить: - обязательно для ввода (<input checked="" type="checkbox"/>) – обязательно присутствие цифр в пароле - опционально (<input type="checkbox"/>) – допускается пароль без цифр
<i>Специальные символы</i>	Перечень спецсимволов, которые могут быть в пароле. Можно установить: - обязательно (<input checked="" type="checkbox"/>) – обязательно присутствие спецсимволов в пароле - опционально (<input type="checkbox"/>) – допускается пароль без спецсимволов

Параметр	Описание
<i>Минимальная длина</i>	Минимально допустимая длина пароля в символах.
<i>Нельзя использовать последние N паролей</i>	Чтобы избежать компрометации, запрещено использовать пароли за предыдущие периоды.
<i>Время действия пароля</i>	Количество дней действия пароля. До истечения указанного срока пароль необходимо сменить.
<i>Период неудачных попыток авторизации</i>	Период (в минутах), в течение которого пользователь может вводить неверный пароль.
<i>Количество неудачных попыток ввода</i>	Количество неуспешных попыток ввода пароля, после которого учетная запись будет заблокирована.
<i>Период блокировки пользователя</i>	Период блокировки учетной записи (в минутах).

3. Нажмите **Сохранить**, чтобы активировать новые параметры. Если нужно вернуться к прежним настройкам, нажмите **Настройки по умолчанию**.

Пример

Период неудачных попыток авторизации – 5.

Количество неудачных попыток ввода – 4.

Период блокировки пользователя – 15.

Если установлены указанные параметры, то после 4 неудачных попыток ввода пароля в течение 5 минут учетная запись пользователя будет заблокирована на 15 минут. После этого можно будет повторить ввод пароля.

Требования к имени пользователя и учетной записи

Имя пользователя должно содержать не менее четырех символов.

Логин пользователя:

- должен начинаться с буквы и не заканчиваться точкой
- может состоять из букв латинского алфавита, арабских цифр и содержать спецсимволы: "_", "-", "=", "."

9.2 Мониторинг состояния Системы


Подсистема мониторинга выполняет проверку работы всех элементов Системы. При этом анализируется доступность элементов распределенной сети, информация об основных аппаратных компонентах, а также информация о состоянии всех служб Системы.

Раздел **Настройки** -> **Состояние системы** содержит следующую информацию:


Поле	Описание
Адрес	IP-адрес ноды Data Discovery
Последнее обновление статуса	Дата и время получения информации о статусе ноды: <ul style="list-style-type: none"> • <i>Ready</i> – доступна и готова к работе; • <i>Not Ready</i> – не готова к работе; • <i>Unknown</i> – зарегистрирована, но не отвечает на запросы.
Версия ядра	Версия ядра ОС
Операционная система	ОС ноды Data Discovery
Память	Общий и занимаемый размер оперативной памяти сервера
ЦПУ	Загрузка центрального процессора сервера Data Discovery
Дисковое пространство (Clickhouse)	Общее выделенное и занятое место на диске для хранения данных БД Clickhouse
Дисковое пространство (PostgreSQL)	Общее выделенное и занятое место на диске для хранения данных БД PostgreSQL
Дисковое пространство (Root)	Общее выделенное и занятое место, отведенное для системных данных в корневой директории
Список всех служб ноды Data Discovery	
Статус	Один из статусов службы: <ul style="list-style-type: none"> • <i>Запущена</i> – работает; • <i>Недоступна</i> – невозможно получить статус; • <i>Не инициализирована</i> – находится в процессе запуска; • <i>Не найдена</i> – должна быть на узле, но отсутствует; • <i>Ошибка</i> – завершена с ошибкой.
Имя	Имя службы в Системе (<i>контейнеры, поды</i>)
Версия	Версия сборки службы
Просмотреть детали	Вывод информации о состоянии, событиях и внутренних сообщениях службы

Все события мониторинга в Системе записываются в журнал.


Чтобы скачать весь журнал:

1. Сформируйте лог-файлы по всем службам. Для этого нажмите  **Экспорт диагностических данных**. После формирования начнется загрузка.
2. Скачайте zip-архив, содержащий txt-файлы с логами.

Чтобы скачать диагностические данные отдельной службы:

1. Нажмите  напротив нужной службы. Начнется формирование лог-файла, а затем загрузка.
2. Скачайте zip-архив, содержащий txt-файлы с логами службы.

10 Настройки продукта

Переход к настройкам осуществляется при нажатии  в правой верхней части экрана. В разделе содержится информация по следующим настройкам Системы:

Экспорт данных - позволяет настроить интеграцию с Traffic Monitor, чтобы отправлять сканированные файлы для анализа.

Хранение - позволяет настроить директории для временного хранения копий скачанных файлов перед тем, как отправить их в Traffic Monitor.

Для настройки см. "InfoWatch Data Discovery. Руководство пользователя", "Интерфейс Data Discovery".