INFOWATCH

InfoWatch Data Discovery. Руководство администратора

13/10/2023

Тел./Факс +7 (495) 229-00-22

http://www.infowatch.ru

СОДЕРЖАНИЕ

Настоящее руководство содержит сведения по настройке InfoWatch Data Discovery (далее Система или Data Discovery) – программного обеспечения, предназначенного для поиска конфиденциальной информации на общих сетевых ресурсах, рабочих станциях, серверах и в хранилищах документов.

1 Аудитория

Данное руководство предназначено для инженеров внедрения и офицеров безопасности, которые будут работать с Системой и заниматься ее администрированием. Руководство рассчитано на пользователей, знакомых с основами работы в среде операционных систем Linux и СУБД PostgreSQL.

2 Комплект документов

В документацию входят:

- «InfoWatch Data Discovery. Руководство по установке». Документ содержит описание процесса установки, обновления и удаления Системы.
- «InfoWatch Data Discovery. Руководство администратора». Документ содержит информацию по настройке Системы.
- «InfoWatch Data Discovery. Руководство пользователя». Содержит описание работы с задачами сканирования.

Сопутствующая документация по системе InfoWatch Traffic Monitor (далее Traffic Monitor) включает в себя:

- «InfoWatch Traffic Monitor. Руководство по установке». Содержит описание 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 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.

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

4 Настройки пользователей

Чтобы перейти к настройкам, нажмите  в правой верхней части экрана. В разделе содержится информация по настройке пользователей Системы и их ролей:

- Пользователи
- Роли

4.1 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
- Добавление нового пользователя из LDAP
- Редактирование учетной записи
- Просмотр профиля пользователя
- Смена пароля пользователя
- Активация и деактивация пользователя
- Удаление пользователя

4.1.1 Создание нового пользователя

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

1. Перейдите в раздел **Настройки пользователей -> Пользователи**.
2. Нажмите **+ Создать**.
3. Выберите **Создать пользователя**.
4. Введите значения параметров согласно таблице:

Параметр	Обязательный параметр	Описание
Фотография	Нет	Фотография пользователя

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

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

4.1.2 Добавление нового пользователя из LDAP

Главный офицер может выбрать из LDAP-каталога новых пользователей, которые также могут выполнять функции Офицеров безопасности. Чтобы добавить нового пользователя в Систему из LDAP-каталога:

1. Перейдите в раздел **Настройки**  -> **Настройки пользователей** -> **Пользователи**.
2. Нажмите **+ Создать**.
3. Выберите **Добавить из LDAP**.
4. Выберите доступный LDAP-сервер, интеграция с которым настроена в Системе (подробнее про интеграцию см. "Интеграция с Active Directory") .
5. В строке поиска начните вводить ФИО или логин пользователя.
6. В результатах поиска выберите нужного пользователя и нажмите **Добавить**.
7. Назначьте пользователю роль (см. подробнее "Редактирование учетной записи").

Пользователь будет добавлен в список пользователей Системы. Новый пользователь входит в Систему с помощью доменных учетных данных. Логин учетной записи имеет вид: `domain\login` или `login@domain`. Для логина учетной записи не учитывается регистр.

> **Примечание:**
>
> Требования к безопасности (см. "Настройки пароля") не распространяются на пользователей, добавленных из LDAP-каталога. Для таких пользователей недоступно изменение пароля в Системе.

> **Важно!**
>
> Изменения учетной записи, внесенные в Active Directory, будут доступны в Системе только после повторного добавления учетной записи: учетную запись необходимо удалить, а затем добавить повторно.

4.1.3 Редактирование учетной записи

Для внесения изменений в учетную запись пользователя:

1. Перейдите в раздел **Настройки пользователей** -> **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. Выберите пользователя.
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**.
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**. Пользователю будет назначена новая роль.

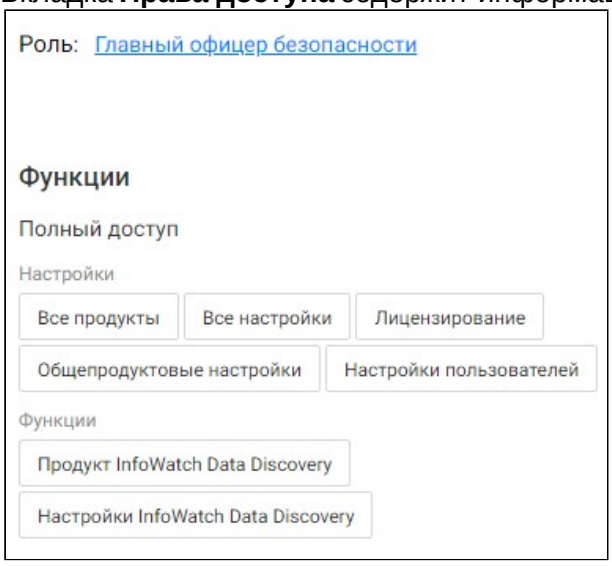
4.1.4 Просмотр профиля пользователя

На странице профиля представлены:

1. 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 .

2. 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;
     - совокупность 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

4.1.5 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 пользователей -> Пользователи** или в профиле пользователя.
2. Выберите **Сменить пароль**.
3. Заполните поля:

Поле	Описание
Старый пароль	Введите действующий пароль

Поле	Описание
Новый пароль	Введите новый пароль. Новый пароль должен удовлетворять настройкам безопасности (см. "Настройки пароля")
Подтверждение пароля	Введите повторно новый пароль

4. Нажмите **Сохранить**.

4.1.6 Активация и деактивация пользователя

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

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

4.1.7 Удаление пользователя

Главный офицер может удалять учетные записи пользователей. Для этого:

1. Перейдите в раздел **Настройки пользователей** -> **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.

4.2 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

4.2.1 Создание и настройка роли

Пользователь Системы с ролью *Главный офицер безопасности* может создавать новые роли и назначать их пользователям. Если у всех пользователей разные компетенции, то для каждого пользователя нужно создать отдельную роль. 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** в списке функций выберите *Продукт InfoWatch Data Discovery*. Пользователю с данной ролью будет предоставлен полный доступ к продукту Data Discovery (по умолчанию доступ запрещен). Если доступ не предоставлен, 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 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.

   Примеры:
   - Если напротив персоны установить  , то эта роль запретит пользователю доступ к любой информации о персоне в Системе.
   - Если напротив персоны установить  (или оставить по умолчанию  у всех персон), то эта роль предоставит пользователю полный доступ к данным персоны.
   - Если напротив персоны установить  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).

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**.

4.2.2 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. 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) – совокупность 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 выбрав необходимую роль из списка.
7. Нажмите **Сохранить**.
8. Для применения настроек пользователь должен выйти из Системы и повторно авторизоваться. Чтобы принудительно завершить сессию пользователей с данной ролью, отметьте ☑ **Завершить активную сессию пользователя** в открывшемся окне, а затем нажмите **Применить**.

4.2.3 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. Выберите роль, которую необходимо удалить для 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 им другую роль.

Чтобы снять роль в карточке пользователя:

1. Перейдите в раздел **Настройки** -> **Настройки пользователей** -> **Пользователи**.
2. Выполните одно из следующих действий:
   - Нажмите на плашке пользователя, для которого необходимо удалить данную роль.
   - Выберите пользователя и 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 активную сессию пользователя**.
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. Выполните одно из следующих действий:
   - Нажмите на плашке пользовательской роли, которую требуется удалить.
   - Выберите роль и 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.

5 Настройки Системы

Чтобы перейти к настройкам, нажмите  в правой верхней части экрана. В разделе содержится информация по следующим настройкам Системы :

- настройка пароля (см. "Настройки пароля");
- состояние Системы (см. "Состояние Системы");
- сбор статистических данных (см. "Основные настройки");
- настройка интеграций с Active Directory (см. "Интеграции").

5.1 Настройки пароля

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 значения параметров:

Параметр	Описание
Буквы	Заглавные и строчные буквы русского и латинского алфавитов, которые используются для составления пароля. Можно установить: - обязательно для ввода (☑) – обязательно присутствие букв в пароле - опционально (☐) – допускается пароль без букв
Цифры	Арабские цифры, которые используются для составления пароля. Можно установить: - обязательно для ввода (☑) – обязательно присутствие цифр в пароле - опционально (☐) – допускается пароль без цифр
Специальные символы	Перечень спецсимволов, которые могут быть в пароле. Можно установить: - обязательно (☑) – обязательно присутствие спецсимволов в пароле - опционально (☐) – допускается пароль без спецсимволов
Минимальная длина	Минимально допустимая длина пароля в символах

Параметр	Описание
Невозможно использование последних N паролей	Чтобы избежать компрометации, запрещено использовать пароли за предыдущие периоды
Срок действия пароля	Количество дней действия пароля. До истечения указанного срока пароль необходимо сменить
Период неудачных попыток авторизации	Период (в минутах), в течение которого пользователь может вводить неверный пароль
Количество неудачных попыток ввода	Количество неуспешных попыток ввода пароля, после которого учетная запись будет заблокирована
Период блокировки пользователя	Период блокировки учетной записи (в минутах)

3. Нажмите **Сохранить**, чтобы активировать новые значения параметров. Если нужно вернуться к прежним настройкам, нажмите **Сбросить настройки до значений по умолчанию**.

> **Пример**
>
> `Период неудачных попыток авторизации – 5.`
>
> `Количество неудачных попыток ввода – 4.`
>
> `Период блокировки пользователя – 15.`
>
> Если установлены указанные значения параметров, 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.

5.1.1 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: "_", "-", "–", "."

5.2 Состояние 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 панели с информацией о нодах Data Discovery. Каждая панель содержит следующую информацию:

Поле	Описание
Лейбл (имя)	Лейбл и имя ноды в формате `лейбл(имя)`
Статус	Статус ноды: • *Ready* – доступна и готова к работе; • *Not Ready* – не готова к работе; • *Unknown* – зарегистрирована, но не отвечает на запросы.
Адрес	IP-адрес ноды Data Discovery
Последнее обновление состояния системы	Дата и время получения информации о статусе ноды
Версия ядра	Версия ядра ОС
Операционная система	ОС ноды Data Discovery
Память	Общий и занимаемый размер оперативной памяти сервера
ЦП	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
Дисковое пространство (NATS)	Общее выделенное и занятое место на диске для хранения данных NATS
Дисковое пространство (Datastorage)	Общее выделенное и занятое место на диске для хранения бинарных данных
Список служб ноды Data Discovery	
Статус	Один из статусов службы:

Поле	Описание
	• *Запущена* – работает; • *Остановлена* – невозможно получить статус; • *Не инициализирована* – находится в процессе запуска; • *Не найдена* – должна быть на узле, но отсутствует; • *Ошибка* – завершена с ошибкой.
Имя	Имя службы в Системе *(контейнеры, поды)*
Версия	Версия сборки службы
Просмотреть детали	Вывод информации о состоянии, событиях и внутренних сообщениях службы

Примечание:

В списке служб не отображаются службы задач сканирования. Чтобы получить лог-файлы выполняющихся задач, экспортируйте диагностические данные.

Все события мониторинга в Системе записываются в журнал.

Чтобы экспортировать диагностические данные:

1. Нажмите **Экспорт диагностических данных**. В диагностические данные будут добавлены лог-файлы работающих служб и лог-файлы выполняющихся задач сканирования со всех нод Data Discovery. После формирования диагностических данных начнется загрузка.

   Примечание:

   Для получения лог-файлов задачи сканирования (например, лог-файлов экземпляров сервиса Puller) убедитесь перед экспортом диагностических данных, что задача запущена.

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.

5.3 Основные настройки

В разделе **Настройки** → **Основные настройки** вы можете управлять сбором статистических данных.

> **Важно!**
>
> Другие настройки этого раздела не используются в текущей версии продукта.

5.3.1 Сбор статистических данных

Система сбора статистики накапливает и обобщает данные о работе пользователя в Консоли управления. По решению пользователя эти данные могут быть скачаны и отправлены в компанию InfoWatch для обработки. Это делается для повышения качества продукта, оценки востребованности той или иной функциональности и разработки новых сценариев работы.

Сбор статистических данных включен по умолчанию. Чтобы отключить сбор данных, снимите флажок в поле **Включить** и нажмите **Сохранить**.

> **Примечание:**
>
> Система сбора статистики не накапливает, не анализирует и не передает персональные данные. Все ФИО пользователей и сотрудников заменяются на внутрисистемные ID-номера.

5.4 Интеграции

В разделе **Настройки** → **Интеграции** вы можете настроить интеграции с Active Directory.

Интеграция с Active Directory позволяет:

- **Добавлять новых пользователей в Систему из LDAP-каталогов**.
  Пользователи, добавленные из LDAP-каталогов, входят в Систему с помощью доменных учетных данных. Подробнее о добавлении пользователя из LDAP-каталога см. "Добавление нового пользователя из LDAP".
  Для добавления нового пользователя из LDAP-каталога не требуется синхронизация.

- **Добавлять хосты из каталога в задачу сканирования** (см. "InfoWatch Data Discovery. Руководство пользователя", "Добавление и настройка хостов").

- **Добавлять в Систему персон и группы из LDAP-каталогов:**
  - В раздел **Досье** будет выгружен список персон с возможностью просмотреть информацию по каждой;
  - Персоны, добавленные из LDAP-каталогов будут иметь тип контакта SID;
  - Система сможет идентифицировать персон и группы по SID. Их имена будут отображаться в таблице с информацией о файлах (см. "InfoWatch Data Discovery. Руководство пользователя", "Таблица с информацией о файлах").

Для добавления данных в Систему требуется провести синхронизацию.

Подробнее о настройке интеграций см. статьи:

- "Интеграция с Active Directory";
- "Редактирование и удаление интеграции".

Важно!

Интеграция с Infowatch Traffic Monitor в разделе **Интеграции** не относится к продукту Data Discovery в текущей реализации.

Для настройки экспорта данных в Traffic Monitor см. "Зоны и серверы".

5.4.1 Интеграция с Active Directory

Чтобы добавить интеграцию с Active Directory:

1. Перейдите в раздел **Настройки** -> **Интеграции**.
2. Нажмите **+ Добавить**.
3. Выберите **Active Directory**.
4. Укажите значения параметров:

Параметр	Описание
Имя интеграции	Название соединения, которое используется в Консоли
Филиал	Лейбл ноды Data Discovery для подключения к Active Directory
Адрес источника	Сетевой адрес сервера Active Directory
Тип соединения	Выбор типа соединения, которое будет установлено: • Незащищенное соединение (Plain) • Защищенное соединение по протоколу LDAP (StartTLS) • Защищенное соединение по протоколу LDAPS (TLS) **Важно:** Соединение без сертификатов небезопасно.
Сертификат	Загрузка файла сертификата в формате PEM или DER Параметр используется, если выбран защищенный тип соединения
Глобальный порт	Порт для подключения глобального LDAP-каталога. По умолчанию используются значения: • 3268 для: • незащищенного соединения (Plain); • защищенного соединения по протоколу LDAP (StartTLS);

Параметр	Описание
	• 3269 для защищенного соединения по протоколу LDAPS (TLS). Чтобы указать значения, используемые по умолчанию, нажмите 
Порт	Порт для подключения локального каталога домена. По умолчанию используются значения: • 389 для: • незащищенного соединения (Plain); • защищенного соединения по протоколу LDAP (StartTLS); • 636 для защищенного соединения по протоколу LDAPS (TLS). Чтобы указать значения, используемые по умолчанию, нажмите 

LDAP-запрос	Атрибуты фильтрации, являющиеся полным путем к указанному каталогу. Может быть указан только один каталог в организационной структуре Active Directory. Для оптимизации поиска вы можете использовать отдельные уровни иерархии базы:
	`C – countryName`
	`O – organizationName`
	`OU – organizationalUnit`
	`DC – domainComponent`
	`CN – commonName`
	Пример: Чтобы использовать в качестве базы поиска ветку Users, расположенную в домене компании, необходимо ввести: `cn=users,dc=company,dc=com`

Логин	Логин для доступа к серверу Active Directory (пользователь должен иметь права на чтение каталога)
Пароль	Пароль для доступа к серверу Active Directory
Синхронизация	Тип синхронизации: ручная или автоматическая. Если выбрана автоматическая синхронизация, то необходимо указать значения в параметрах **Периодичность** и **Повторение**
Периодичность	Интервал проведения автоматической синхронизации. Например, если у параметра **Периодичность** значение **Ежечасно** и у параметра **Повторение** значение **2**, то синхронизация запускается с интервалом в 2 часа.
Повторение	

5. Нажмите **Проверить соединение**, чтобы проверить, что все параметры заполнены корректно, и дождитесь сообщения **Соединение успешно установлено**. В случае появления статуса:
    - **Не удалось установить соединение** – проверьте, что были введены корректные адрес и порт;
    - **Заданы неверные логин или пароль** – проверьте, что были введены корректные логин и пароль.
6. Нажмите:
    - **Сохранить** – чтобы сохранить интеграцию без проведения синхронизации;
    - **Сохранить и синхронизировать** – чтобы сохранить интеграцию и запустить процесс синхронизации немедленно.

> **Важно!**
>
> Синхронизация с Active Directory может создавать высокую нагрузку на сервера домена и сеть, поэтому рекомендуется проводить первую синхронизацию с Active Directory в ночное время.

Интеграция будет добавлена в Систему. Чтобы запустить синхронизацию вручную , нажмите  на панели интеграции.

Информация о интеграциях

Каждая интеграция отображается в отдельной панели.

В нижней строке панели указано:

-  – количество добавленных в ходе синхронизаций персон, групп и рабочих станций;
-  – количество персон, групп и рабочих станций, данные которых обновились в ходе последней синхронизации.

Для каждой интеграции указывается статус синхронизации:

Статус	Описание
НЕ СИНХРОНИЗИРОВАЛОСЬ	Интеграция сохранена, синхронизация еще не разу не запускалась
СИНХРОНИЗИРУЕТСЯ	Идет процесс синхронизации
УСПЕШНО	Синхронизация завершилась успешно
ПРЕРВАНА	Синхронизация остановлена пользователем. В статусе также указаны дата и время остановки

Статус	Описание
ОШИБКА	Данный статус может обозначать следующее: • введены некорректные логин, пароль, или адрес; • в ходе синхронизации произошла ошибка.

5.4.2 Редактирование и удаление интеграции

Чтобы внести изменения в уже созданную интеграцию:

1. Нажмите  в правом верхнем углу и выберите **Редактировать**.
2. Внесите изменения.
3. Нажмите **Сохранить**:
    - Чтобы создать новую интеграцию с указанными настройками вместо текущей интеграции, нажмите **Создать новую**. Текущая интеграция будет удалена.
    - Если требуется изменить настройки интеграции, нажмите **Продолжить в этой**.

Чтобы удалить интеграцию:

1. Нажмите  в правом верхнем углу.
2. Выберите **Удалить**, затем нажмите **Ок**.

> **Примечание:**
>
> Данные, полученные в результате синхронизаций, не будут удалены после удаления интеграции.

6 Лицензирование

В разделе **Настройки** → **Лицензирование** вы можете управлять лицензиями.

Запуск задач сканирования доступен, только если в Системе есть активная лицензия.

6.1 Пробная лицензия

По умолчанию в Систему добавлена пробная лицензия сроком на один месяц. Дата установки продукта является датой начала действия для этой лицензии.

6.2 Действия с лицензиями

Чтобы добавить лицензию:

1. Нажмите **+Добавить**;
2. В открывшемся окне добавьте файл лицензии.

Чтобы удалить лицензию:

1. В углу плитки лицензии нажмите ;
2. Выберите **Удалить**;
3. Нажмите **Ок**.

7 Зоны и серверы

В разделе **Настройки** → **Настройки продукта** → **Зоны и серверы** вы можете управлять зонами и серверами Data Discovery.

Зона – группа серверов Data Discovery. Разделение серверов на зоны позволяет:

- Запускать сервисы задач только на определенных серверах. В зону могут входить несколько серверов из кластера Системы. Каждый сервер может входить только в одну зону.
- Настраивать экспорт данных в Traffic Monitor для каждой группы серверов. Каждая зона имеет отдельные настройки для экспорта данных.

Вы можете выбрать зону задачи сканирования в настройках задачи (см. "InfoWatch Data Discovery. Руководство пользователя", "Создание, настройка и запуск задачи").

7.1 Управление зонами

На вкладке **Зоны**:

- Слева отображается список зон.
- В рабочей области справа отображаются настройки экспорта данных в Traffic Monitor и список серверов зоны.

7.1.1 Создание

Чтобы создать зону:

1. Перейдите на вкладку **Зоны**.
2. Нажмите **Создать зону**.
3. Введите имя зоны.
4. Нажмите **Создать**.

7.1.2 **Переименование**

Чтобы переименовать зону:

1. Перейдите на вкладку **Зоны**.
2. Слева отображается список зон. Нажмите справа от имени зоны.
3. Выберите **Переименовать**.
4. Введите новое имя зоны.
5. Нажмите **Сохранить**.

7.1.3 **Удаление**

Если вы удалите зону, сервера будут удалены из зоны. Система на серверах не будет удалена.

Вы не можете удалить зону, если зона выбрана в задачах. Измените зону в настройках задач или удалите такие задачи.

Вы не можете удалить предустановленную зону **По умолчанию**.

Чтобы удалить зону:

1. Перейдите на вкладку  **Зоны**.
2. Слева отображается список зон. Нажмите  справа от имени зоны.
3. Выберите  **Удалить**.
4. Нажмите **Удалить**.

7.1.4 Добавление серверов в зону

Чтобы добавить серверы в зону:

1. Перейдите на вкладку  **Зоны**.
2. Слева отображается список зон. Выберите зону.
3. Нажмите  **Добавить сервер** в рабочей области справа.
4. В открывшемся окне отображаются серверы, которые не добавлены ни в одну зону. Выберите серверы.
5. Нажмите **Добавить**.
6. Перезапустите задачи в зоне, чтобы сервисы задач могли запускаться на добавленных серверах.

7.1.5 Экспорт данных в Traffic Monitor

Чтобы отправлять копии файлов и информацию о файлах в Traffic Monitor для анализа в процессе выполнения задачи сканирования, настройте экспорт данных. Для экспорта данных необходимы плагин и лицензия Traffic Monitor (см. "Плагин и лицензия Traffic Monitor").

Чтобы настроить экспорт данных:

1. Перейдите на вкладку  **Зоны**.
2. Слева отображается список зон. Выберите зону
3. Разверните панель **Экспорт данных в Traffic Monitor**.
4. Укажите значения параметров:
   a. **Версия ТМ**:
   Версия Traffic Monitor на сервере, к которому необходимо подключиться. Выберите **Версия 6.10** или **Версия 7.1 и выше**.

   > **Примечание:**
   >
   > Чтобы узнать номер версии ТМ, перейдите в Консоли управления Traffic Monitor в раздел **Офицер безопасности** → **О системе**.

   b. **Адрес XAPI**:
   Адреса XAPI серверов Traffic Monitor. Серверы должны входить в один кластер Traffic Monitor. Data Discovery отправляет данные на серверы из списка.
   - Чтобы добавить адрес:
     i. Введите адрес в формате IP-адреса IPv4: "xxx.xxx.xxx.xxx".
     ii. Нажмите Enter.

- Вы можете указать несколько адресов. Если один адрес недоступен, Система автоматически начинает использовать следующий указанный адрес.
- Traffic Monitor версии 7.7 или выше сообщает, если на сервере недостаточно места для получения данных от Data Discovery (см. "Traffic Monitor. Справочник по конфигурационным файлам", параметры `FreeSpaceThresholdMountPoint` и `FreeSpaceThresholdGb` в **xapi.conf**). В этом случае Data Discovery переключается на следующий адрес XAPI или повторно пытается отправить данные через 1 минуту.

c. **Токен**:
Токен для подключения.

> **Примечание:**
>
> Чтобы скопировать токен для подключения:
>
> i. В Консоли управления Traffic Monitor перейдите в раздел **Управление** -> **Плагины**.
> ii. Выберите в левой верхней части экрана предустановленный плагин:
> - "InfoWatch Crawler" для Traffic Monitor версии 7.3 и ниже;
> - "InfoWatch Data Discovery" для Traffic Monitor версии выше 7.3.
>
> iii. Скопируйте предоставленный токен, нажав  .

5. Нажмите **Применить**.
6. Перезапустите задачи в зоне. Задачи получат новые настройки экспорта данных при запуске.

7.2 Управление серверами

На вкладке  **Серверы** отображается список всех серверов Data Discovery. Список серверов для каждой зоны отображается на вкладке  **Зоны**.

На панели сервера отображается следующая информация:

Данные сервера	Описание
 Имя	Лейбл и имя сервера в формате: `лейбл(имя)`
 Зона	Зона, в которую добавлен сервер. Значение отсутствует, если сервер не добавлен зону. • Если вы устанавливаете Систему в режиме центрального офиса или обновляете центральный офис до версии 1.7, то сервер центрального офиса автоматически добавляется в зону **По умолчанию**. • Сервера филиалов не добавляются в зоны автоматически после установки/обновления Системы.

Данные сервера	Описание
 Роль	В текущей версии Системы все сервера имеют роль **Сканер и передатчик**
 Хранилище	Данные о пространстве в хранилище сервера

7.2.1 Выбор зоны и удаление из зоны

Примечание:

Вы не можете изменить зону сервера или удалить сервер из зоны, если в хранилище сервера есть файлы задач.

Чтобы получить количество файлов задач в хранилище сервера:

1. Подключитесь к ssh-консоли сервера. Файлы задач хранятся в директориях `PATH/NUMBER`, где:
   - `PATH` – путь к хранилищу сервера, по умолчанию: `/mnt/disctps`;
   - `NUMBER` – номер задачи сканирования.
2. Выполните команду `ls PATH/NUMBER -1 | wc -l` для каждой задачи. Пример: `ls /mnt/disctps/7 -1 | wc -l`

Чтобы удалить файлы из хранилища, выполните одно из действий для каждой задачи в хранилище:

- Отправьте файлы задачи в Traffic Monitor:
  1. В настройках задачи:
     - Отключите параметр **Собирать только информацию о файлах**.
     - В настройках задачи укажите следующие значения:
       - **0** для параметра **Число сканеров**;
       - **N** для параметра **Число передатчиков**, где **N** больше или равно количеству серверов Data Discovery в зоне задачи.
  2. Запустите задачу. Система отправляет файлы в Traffic Monitor и удаляет их из хранилищ, но не скачивает новые файлы в хранилища зоны.
  3. Дождитесь, когда в хранилище не останется файлов задачи.
  4. Остановите задачу.
- Удалите задачу. Файлы будут удалены и не будут отправлены в Traffic Monitor.

Чтобы добавить сервер в зону / изменить зону сервера:

1. Нажмите  на панели сервера.
2. Выберите  **Выбрать зону**.
3. Выберите зону в списке.

4. Нажмите **Применить**.
5. Перезапустите задачи в новой зоне сервера, чтобы сервисы задач могли запускаться на этом сервере.

Чтобы удалить сервер из зоны:

1. Нажмите ⋮ на панели сервера.
2. Выберите 🗑 **Удалить из зоны**.
3. Нажмите **Удалить**. Система на сервере не будет удалена.

7.2.2 Настройка хранилища

Каждый сервер Data Discovery имеет хранилище для просканированных файлов. Все серверы имеют одинаковый путь для хранилища (по умолчанию: `/mnt/disctps`). Путь для хранилища указывается при установке Системы на центральном офисе.

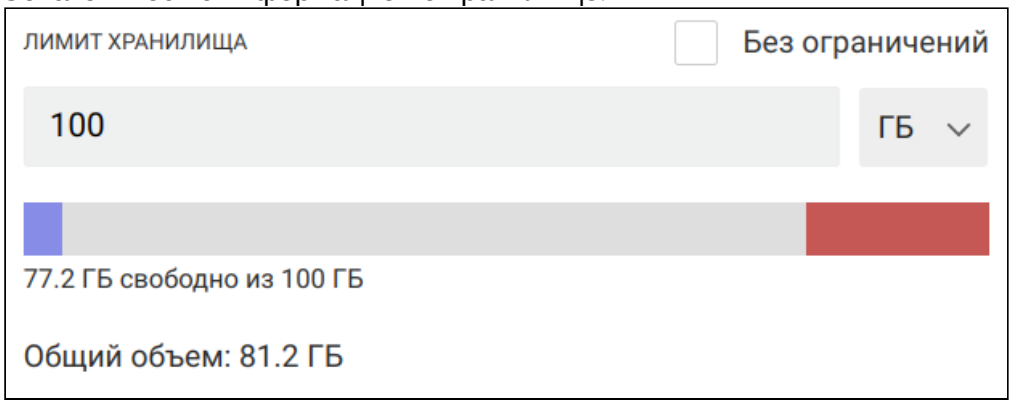
> **Примечание:**
>
> Рекомендуется, чтобы хранилище сервера находилось в отдельном разделе или диске.

> **Важно!**
>
> В хранилище должны находиться только файлы и директории, которые были добавлены Системой. Если вы добавите другие файлы или директории в хранилище, Система может работать некорректно.

Во время сканирования Система скачивает файл в одно из хранилищ зоны. Файл удаляется из хранилища после отправки в Traffic Monitor.

Чтобы настроить хранилище:

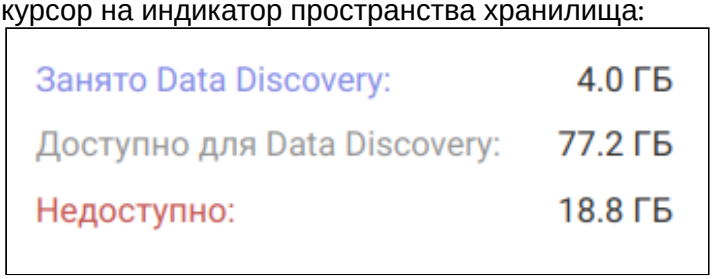
1. Нажмите ⋮ на панели сервера.
2. Выберите ⚙ **Настроить роли.**
3. Ознакомьтесь с информацией о хранилище:



- В поле **Лимит хранилища** указан текущий лимит.
- Если включена настройка **Без ограничений**, то лимит хранилища не используется.

- **Общий объем** = свободное пространство на диске + пространство, которое занято файлами Data Discovery.

4. Чтобы просмотреть подробную информацию о пространстве в хранилище, наведите курсор на индикатор пространства хранилища:



   - **Занято Data Discovery** – пространство, которое занято файлами Data Discovery.
   - **Доступно для Data Discovery** – свободное пространство на диске, которое Data Discovery может использовать.
   - **Недоступно** – отображается, если лимит превышает **Общий объем** хранилища.

5. Настройте лимит:

> **Важно!**
>
> Установите лимит для хранилища, если Система и хранилище расположены в одном разделе. Рекомендуется настроить лимит так, чтобы в разделе всегда было доступно 10 ГБ.
>
> Система может работать некорректно, если в разделе недостаточно свободного места.

   - Чтобы установить лимит:
     a. Отключите настройку **Без ограничений**.
     b. Укажите лимит в поле **Лимит хранилища** и выберите единицу измерения. Система остановит загрузку файлов в хранилище, если занятое место в хранилище достигнет лимита. Если место освободится, Система продолжит загрузку.
   - Если лимит не требуется, включите настройку **Без ограничений**. Система остановит загрузку файлов в хранилище, если закончится свободное место на диске. Если место освободится, Система продолжит загрузку.

6. Нажмите **Применить**. Система начнет использовать новые настройки хранилища.

8 Плагин и лицензия Traffic Monitor

Для экспорта данных из Системы в Traffic Monitor необходимы плагин и лицензия Traffic Monitor.

Об установке лицензии в Traffic Monitor см. "InfoWatch Traffic Monitor. Руководство пользователя", раздел "Управление лицензиями".

Для экспорта данных используйте предустановленный плагин в Консоли управления Traffic Monitor:

- "InfoWatch Crawler" для Traffic Monitor версии 7.3 и ниже;
- "InfoWatch Data Discovery" для Traffic Monitor версии выше 7.3.

Плагин отображается, только если в Traffic Monitor установлена действующая лицензия.

Информация о плагине будет доступна в разделе **Управление** → **Плагины** в Консоли управления Traffic Monitor. Для последующей отправки данных в Traffic Monitor необходим токен, который создается автоматически и доступен в разделе **Управление** → **Плагины** → **Токены**.

Подробнее о настройке экспорта данных см. "Зоны и серверы".

9 Добавление пользовательского сертификата

Чтобы не допустить несанкционированный доступ к Системе и повысить защищенность канала передачи данных, можно добавить новый пользовательский сертификат для web-службы. Это действие доступно в любой момент использования Системы и выполняется через командную строку. Чтобы добавить пользовательский сертификат:

1. Разместите на диске два файла в формате PEM:
   - файл с сертификатом (например: `test.crt`);
   - файл с закрытым ключом (например: `test.key`)
2. Перейдите в директорию, в которую был распакован архив с дистрибутивом при установке Системы.
3. Выполните команду от имени пользователя с правами root:
   `./setup.py setwebkeys --certificate=/folder/test.crt --privatekey=/folder/test.key`

   В нашем примере:
   - `/folder/test.crt` – полный путь к файлу с сертификатом;
   - `/folder/test.key` – полный путь к файлу с закрытым ключом.

Последний добавленный сертификат считается действительным. После добавления или замены сертификата обновите вручную все открытые вкладки браузера, используемые Системой.

10 Ротация лог-файлов

10.1 Сервисы задач сканирования

Для выполнения задач сканирования Система использует сервисы: Puller, Sender, Task Execution Controller. Лог-файлы экземпляров сервисов хранятся в поддиректориях директории `/var/log/infowatch/disc` на сервере, где были запущены сервисы задачи сканирования.

При каждом запуске задачи Система добавляет в директорию `/var/log/infowatch/disc` поддиректорию для каждого экземпляра сервиса, участвующего в выполнении задачи. В поддиректорию добавляются лог-файлы экземпляра сервиса. Каждая поддиректория имеет уникальный идентификатор в ее названии.

10.2 Сервис Discoperator

В директории `/var/log/infowatch/disc` на центральном офисе хранятся лог-файлы сервиса Discoperator. Этот сервис используется для работы Консоли управления.

Сервис функционирует постоянно и добавляет записи в лог-файл. Если сервис был перезапущен, то Система добавляет в директорию `/var/log/infowatch/disc` поддиректорию для нового экземпляра сервиса.

10.3 Сервис TPS Agent

В директории `/var/log/infowatch/disc` на каждом сервере хранятся лог-файлы сервиса TPS Agent. Этот сервис используется для управления хранилищем сервера.

Сервис функционирует постоянно и добавляет записи в лог-файл. Если сервис был перезапущен, то Система добавляет в директорию `/var/log/infowatch/disc` поддиректорию для нового экземпляра сервиса.

10.4 Ротация лог-файлов

Экземпляры сервисов добавляют большое количество записей в лог-файлы. Размер лог-файлов постоянно растет, что приводит к уменьшению свободного дискового пространства.

Освободить дисковое пространство можно следующими способами:

- Остановить все задачи сканирования в Консоли управления, после чего удалить поддиректории и лог-файлы вручную из директории `/var/log/infowatch/disc`. При повторном запуске задачи Система:
  - создает новые поддиректории с новыми идентификаторами;
  - создает в поддиректориях лог-файлы, в которые будут добавляться записи о выполнении задачи.

> **Важно!**
>
> Если удалить лог-файлы у выполняющейся задачи, то записи не будут сохраняться в Системе, пока задача не будет остановлена и запущена повторно.

Важно!

Не рекомендуется удалять вручную директории и лог-файлы запущенных сервисов Discoperator и TPS Agent. Директории этих сервисов имеют имена вида:

- `discoperator-central-5c5769b58d-77rq2`
- `tps-agent-f85x8`

- Настроить ротацию лог-файлов.

Для регулярного и автоматического удаления устаревших записей рекомендуется настроить ротацию лог-файлов. Ротация лог-файлов – автоматический процесс для управления лог-файлами. При ротации в зависимости от настроек могут выполняться следующие действия:

- Создание нового файла, который является версией оригинального лог-файла. В новый файл перемещаются записи из оригинального лог-файла.
- Сжатие версий оригинального лог-файла.
- Удаление устаревших файлов.

10.5 Настройка ротации с помощью logrotate и crontab

Настройка ротации требуется на центральном офисе и на каждом сервере Data Discovery, на котором будут запускаться сервисы задачи сканирования.

Чтобы настроить ротацию лог-файлов на сервере:

Важно!

Все действия необходимо выполнять от имени пользователя с правами root.

1. Настройте утилиту **logrotate**:
   a. Проверьте содержимое конфигурационного файла **`/etc/logrotate.conf`**
   Конфигурационный файл должен содержать следующую строку:
   `include /etc/logrotate.d`
   Добавьте указанную строку в конфигурационный файл, если строка отсутствует.
   b. В директории **`/etc/logrotate.d`** создайте файл для конфигурации logrotate для Data Discovery (в нашем примере имя файла – **`iwdd`**).
   c. Откройте созданный файл для редактирования и укажите в файле следующую конфигурацию:

iwdd

```
/var/log/infowatch/disc/*/*.log {
    daily
    copytruncate
    rotate 7
    notifempty
    compress
    missingok
}
```

Описание конфигурации

Содержимое	Описание
/var/log/infowatch/disc/*/*.log {	производить ротацию лог-файлов в поддиректориях директории `/var/log/infowatch/disc`
daily	производить ротацию ежедневно
copytruncate	во время каждой ротации создавать версию для каждого оригинального лог-файла, после чего перемещать все записи из оригинального файла в созданную версию
rotate 7	для каждого оригинального лог-файла хранить 7 последних версий, удалять более старые версии лог-файла
notifempty	не производить ротацию, если в оригинальном лог-файле нет записей
compress	производить сжатие каждой версии оригинального лог-файла
missingok	не сообщать об ошибке, если оригинальный лог-файл не был обнаружен
}	

d. Сохраните внесенные изменения. По умолчанию logrotate запускается автоматически ежедневно с помощью cron.
e. Чтобы проверить корректность конфигурации без проведения ротации, выполните команду:
`logrotate -d /etc/logrotate.d/iwdd`

2. Если экземпляр сервиса был перезапущен, то новый экземпляр добавляет записи в новый лог-файл в новой поддиректории. Старый файл после одной ротации станет пустым и больше не будет подлежать ротации. Настройте автоматическое удаление неиспользуемых файлов и поддиректорий с помощью файла **crontab**:
   a. Откройте для редактирования файл `crontab` для пользователя root, выполнив команду:
   `crontab -u root -e`
   b. Добавьте в конфигурационный файл одну строку:

```
30 5 * * * find /var/log/infowatch/disc/ -mtime +7 -name "*.log*" -delete > /dev/
null 2>&1; find /var/log/infowatch/disc/ -empty -type d -delete > /dev/null 2>&1
```

Указанный скрипт выполняется ежедневно в 5:30. Скрипт последовательно выполняет следующие действия:
   i. Удаляет из поддиректорий лог-файлы и версии лог-файлов, которые были изменены более 7 дней назад.

ii. Удаляет пустые поддиректории.

c. Сохраните изменения. Скрипт будет автоматически запускаться ежедневно с помощью cron.

В результате настройки:

- logrotate регулярно осуществляет ротацию лог-файлов Data Discovery и удаляет устаревшие версии лог-файлов;
- скрипт, указанный в crontab, регулярно удаляет неиспользуемые файлы и пустые поддиректории.